ПЛАН ДЕЙСТВИЙ, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ И (ИЛИ) ВОССТАНОВЛЕНИЕ ДЕЯТЕЛЬНОСТИ БАНКА В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕСТАНДАРТНЫХ И ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

1. Основные понятия и определения

1.1. Для целей настоящего Плана действий, направленных на обеспечение непрерывности и (или) восстановления деятельности Банк в случае возникновения нестандартных и чрезвычайных ситуаций (далее – план ОНиВД), используются следующие основные понятия, определения и сокращения:

- *банк* – Банк, в том числе головной офис, обособленные структурные подразделения;
- *бизнес-процесс* – логически законченная последовательность действий и (или) операций, в совокупности реализующих конкретную задачу текущей деятельности, описываемая формальным алгоритмом преобразования на каждом этапе входных элементов в выходные. К элементам преобразования могут относиться документы или ресурсы разной природы и назначения (финансовые, материальные и нематериальные активы);
- *головной офис банка (ГО)* – месторасположение органов управления банком, а также его структурных подразделений по месту его государственной регистрации (г. Москва), за исключением внутренних структурных подразделений банка;
- *ГУЧС* – группа управления в чрезвычайных ситуациях;
- *критические операции* – важные внутренние банковские процессы (сферы деятельности банка), непрерывность деятельности которых определяет возможность банка осуществлять банковские операции и выполнять в установленные сроки и в установленных размерах обязательства перед клиентами;
- *нестандартные и чрезвычайные ситуации (НЧС)* – это условия или ситуации, обусловленные действием обстоятельств непреодолимой силы, т. е. чрезвычайных и непредотвратимых при данных условиях обстоятельств, возникших помимо воли и желания сотрудников банка, которые нельзя было предвидеть или избежать и конечный результат которых будет подтверждён только при совершении или несовершении одного или более действий, предусмотренных настоящим планом ОНиВД;
- *обособленные структурные подразделения* – подразделения банка (филиалы), непосредственно занимающеися совершением банковских операций, их оформлением и учётом вне места нахождения головного офиса;
- *план обеспечения непрерывности деятельности и (или) восстановления деятельности банка в случае возникновения нестандартных и чрезвычайных ситуаций* – комплекс мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования банка, вызванного нестандартными и чрезвычайными ситуациями (возникновением чрезвычайной ситуации или иным событием, наступление которого возможно, но труднопредсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению банком принятых на себя обязательств);
- *регуляторный (комплаенс) риск* – риск возникновения у банка прямых или косвенных потерь из-за несоблюдения законодательства РФ, внутренних нормативных документов банка, стандартов саморегулируемых организаций или

иных стандартов, которые банк в своих внутренних нормативных документах или договорах определяет как обязательные для себя, а также в результате применения санкций и (или) иных мер воздействия со стороны надзорных органов;

- *резервное помещение* – постоянно действующая и поддерживаемая в рабочем состоянии организационно-техническая структура банка, обеспечивающая выполнение необходимых функций в случае наступления нестандартных и чрезвычайных ситуаций;
- *структурное подразделение* – внутреннее подразделение банка, непосредственно занимающееся совершением банковских операций, их оформлением и учётом.

2. Общие положения

2.1. План ОНиВД является внутренним нормативным документом банка, устанавливает порядок взаимодействия подразделений в случае возникновения нестандартных и чрезвычайных ситуаций в целях оперативного решения вопросов по обеспечению непрерывности и (или) восстановлению деятельности банка и разработан с учётом требований:

- Федерального закона от 02.12.90 № 395-1 «О банках и банковской деятельности»;
- Федерального закона от 21.12.94 № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»;
- Федерального закона от 12.02.98 № 28-ФЗ «О гражданской обороне»;
- Федерального закона от 21.12.94 № 69-ФЗ «О пожарной безопасности»;
- Федерального закона от 27.06.11 № 161-ФЗ «О национальной платёжной системе»;
- Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных»;
- Федерального закона от 07.08.01 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма»;
- постановления Правительства РФ от 21.05.07 № 304 «О классификации чрезвычайных ситуаций природного и техногенного характера» (далее – постановление № 304);
- постановления Правительства РФ от 04.09.03 № 547 «О подготовке населения в области защиты от чрезвычайных ситуаций природного и техногенного характера»;
- постановления Правительства РФ от 02.11.2000 № 841 «Об утверждении Положения об организации подготовки населения в области гражданской обороны»;
- постановления Правительства РФ от 25.04.12 № 390 «О противопожарном режиме»;
- Положения Банка России от 16.12.03 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах»;
- постановления Правительства Москвы от 24.02.09 № 124-ПП «Об организации планирования действий по предупреждению и ликвидации чрезвычайных ситуаций»;
- Положения Банка России от 09.06.12 № 382-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»;
- иных требований и рекомендаций Банка России, в том числе распоряжений и стандартов в области обеспечения информационной безопасности банковской системы РФ;
- письма Банка России от 24.05.05 № 76-Т «Об организации управления

операционным риском в кредитных организациях»;
- программы курсового обучения сотрудников в области гражданской обороны и предотвращения чрезвычайных ситуаций в Банк;
- программы вводного инструктажа по гражданской обороне и предотвращению чрезвычайных ситуаций в Банк;
- иных внутренних документов банка.

2.2. План ОНиВД определяет основные принципы и методы обеспечения непрерывности деятельности банка при возникновении различных нестандартных и чрезвычайных ситуаций, устанавливает задачи, порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима повседневного функционирования банка, вызванного нестандартной и чрезвычайной ситуацией.

План является частью системы внутреннего контроля банка в области снижения уровня специфических и неспецифических рисков, в том числе операционного риска.

2.3. Обособленные структурные подразделения банка разрабатывают собственный план ОНиВД, руководствуясь принципами, заложенными в настоящем плане ОНиВД, с учётом своей специфики функционирования и возможных НЧС, присущих в регионе местонахождения обособленного структурного подразделения банка.

2.4. В случае принятия новых или изменения действующих законодательных и нормативно-правовых актов, регулирующих подходы к обеспечению непрерывности деятельности банка, план ОНиВД до внесения соответствующих изменений и дополнений действует в части, им не противоречащей.

2.5. В случае изменения наименований структурных подразделений и (или) должностей сотрудников банка, участвующих в осуществлении мероприятий (процедур) в рамках плана ОНиВД, при условии сохранения за ними функций, определённых для данных структурных подразделений и сотрудников банка планом ОНиВД, а также в случае передачи указанных функций в компетенцию других структурных подразделений и сотрудников банка работа в соответствии с планом ОНиВД осуществляется соответствующими структурными подразделениями и сотрудниками банка до внесения изменений в план ОНиВД.

2.6. Настоящий план ОНиВД, а также все изменения и дополнения к нему утверждаются наблюдательным советом банка.

3. Цели и задачи плана ОНиВД

3.1. План ОНиВД - перечень мероприятий, которые должны быть выполнены в целях предотвращения наступления и после возникновения нестандартных и чрезвычайных ситуаций.

3.2. Планирование обеспечения непрерывности деятельности и (или) восстановления деятельности банка в случае возникновения нестандартных и чрезвычайных ситуаций осуществляется в целях:

- предотвращения наступления нестандартных и чрезвычайных ситуаций, предупреждения и предотвращения возможного нарушения режима повседневного функционирования банка;

- обеспечения безопасности и соответствующих условий труда сотрудников банка, безопасности лиц, находящихся в помещениях (посетителей) банка;
- повышения готовности сотрудников банка к умелым и адекватным действиям при угрозе и возникновении опасностей, присущих чрезвычайной ситуации и военным конфликтам, характерным для района работы и проживания сотрудников банка;
- снижения тяжести последствий нарушения режима повседневного функционирования банка (в том числе размера материальных потерь, потерь информации, потери деловой репутации);
- сведения к минимуму воздействия аварий на бизнес-процессы банка, поддержания способности банка выполнять принятые на себя обязательства перед вкладчиками и кредиторами, в том числе перед Банком России (по кредитам Банка России, уплате процентов по ним и другим денежным обязательствам перед ЦБ РФ);
- сохранения уровня управления банком, позволяющего обеспечить условия для принятия обоснованных и оптимальных управленческих решений, их своевременную и полную реализацию;
- уменьшения отрицательных последствий происшествий для стратегии развития банка, его репутации, ликвидности, качества кредитов и позиции на рынке;
- уменьшения юридической ответственности банка и способности соблюдать все нормативные требования и законы;
- обеспечения информационной безопасности банка, в том числе его расчётной системы;
- обеспечения бесперебойной работы банка как расчётного центра платёжной системы «Мультисервисная платёжная система»;
- организованного восстановления деятельности банка;
- улучшения репутации банка и получения конкурентных преимуществ в случае успешного обеспечения непрерывности деятельности в чрезвычайных ситуациях.

3.3. В целях обеспечения непрерывности деятельности и (или) восстановления деятельности банка в случае возникновения нестандартных и чрезвычайных ситуаций решаются следующие задачи:

- контроля за соблюдением действующих правил сохранности и доступа к необходимой информации;
- обеспечения персонала рабочими помещениями, своевременного перемещения персонала из помещения, где произошло чрезвычайное событие, в безопасное резервное помещение;
- обеспечения персонала техническими средствами и необходимыми материалами;
- организации непрерывного выполнения банком своих обязательств перед клиентами при чрезвычайном событии;
- обеспечения взаимодействия с акционерами, бизнес-партнёрами, подрядчиками, поставщиками и другими заинтересованными сторонами;
- профилактики возникновения непредвиденных обстоятельств на основе осведомлённости персонала о мерах технической, информационной и пожарной безопасности;
- снижения риска гибели персонала и клиентов банка и уничтожения имущества банка в результате возникновения нестандартных и чрезвычайных ситуаций;
- снижения возможного воздействия опасных факторов, возникших вследствие возникновения непредвиденных обстоятельств (чрезвычайной ситуации);
- сокращения времени ликвидации последствий возникновения нестандартных и чрезвычайных ситуаций;
- разграничения полномочий и обязанностей персонала банка в процессе ликвидации

чрезвычайных ситуаций;
- восстановления доступа к необходимой информации.

3.4. В целях реализации задач план ОНиВД:

- определяет последовательность действий в случае возникновения чрезвычайных ситуаций и порядок осуществления внутренних банковских процессов в чрезвычайном режиме;
- определяет порядок документирования согласованных решений, перечень процедур, выполнение которых в режиме повседневного функционирования банка необходимо для успешной реализации плана, очерёдность и сроки их выполнения;
- содержит перечень процедур и изложение способов реагирования на нестандартные и чрезвычайные ситуации для сотрудников банка (в том числе детальные инструкции), выполнение которых позволит осуществлять критические операции, минимизировать возможный ущерб и в минимально короткие сроки восстановить нормальную работу банка и (или) его обособленных структурных подразделений;
- устанавливает порядок реализации указанных решений и процедур;
- определяет документирование распределения и перераспределения обязанностей должностных лиц банка и (или) его обособленных структурных подразделений по обеспечению исполнения указанных решений в условиях чрезвычайного режима с учётом взаимозаменяемости сотрудников банка в случае отсутствия (недоступности) ответственных и (или) уполномоченных сотрудников банка;
- устанавливает порядок взаимодействия между органами управления, структурными подразделениями, обособленными структурными подразделениями и сотрудниками банка при возникновении нестандартных и чрезвычайных ситуаций;
- устанавливает порядок информирования заинтересованных лиц о возникновении нестандартных и чрезвычайных ситуаций, порядок взаимодействия с ними, в том числе с ЦБ РФ, по вопросам обеспечения непрерывности и (или) восстановления деятельности банка;
- определяет организацию и порядок осуществления обучения сотрудников банка;
- устанавливает требования к уровню знаний и умений сотрудников банка;
- определяет порядок завершения работы в чрезвычайном режиме и возврата в режим повседневного функционирования.

3.5. Обеспечение непрерывности деятельности банка реализуется на основе:

- вовлечённости сотрудников банка в процесс обеспечения непрерывности деятельности за счёт их обучения, осведомлённости о целях банка в области обеспечения непрерывности деятельности;
- ознакомления сотрудников банка с порядком обеспечения непрерывности деятельности банка и осознания важности его соблюдения;
- понимания сотрудниками банка того, что процесс обеспечения непрерывности деятельности не является окончательным и неизменным, что он должен и будет непрерывно улучшаться и совершенствоваться в соответствии с новыми условиями как внутри банка, так и за его пределами;
- участия сотрудников банка в совершенствовании процесса обеспечения непрерывности деятельности банка.

4. Классификация категорий и видов угроз непрерывности деятельности банка

4.1. Определение нестандартных и чрезвычайных ситуаций и объекта риска

4.1.1. Непредвиденное обстоятельство (чрезвычайная ситуация) - это обстановка, сложившаяся в результате аварии, опасного природного явления, катастрофы, стихийного или иного бедствия, которые могут повлечь или повлекли за собой человеческие жертвы, ущерб здоровью людей или окружающей среде, значительные материальные потери и нарушение условий жизнедеятельности людей. Непредвиденные обстоятельства приводят к невозможности функционирования банка в обычном, регламентируемом соответствующими стандартами банка режиме.

4.1.2. Объект риска - персонал, клиенты, бизнес-процесс, вид деятельности, имущество и информационные активы банка.

4.1.3. Категория (или тип) нестандартных и чрезвычайных ситуаций – это основная классификация угроз непрерывности деятельности банка.

4.2. Классификация категорий (типов) нестандартных и чрезвычайных ситуаций

4.2.1. Непредвиденные обстоятельства (чрезвычайные ситуации) классифицируются по их источникам. В целях обеспечения непрерывности бизнес-процессов банком признаются существенными следующие виды рисков прерывания деятельности:

4.2.1.1. предпринимательский:

- переезд банка в другое помещение или офис;
- промышленный шпионаж;
- утрата архива;
- слияние банка с другими банками или приобретение (поглощение) других банков;
- попытка рейдерского захвата бизнеса;
- переход с одной автоматизированной банковской системы на другую;
- чрезмерная зависимость от партнёров (клиентов);
- ошибки, допущенные при заключении контрактов с провайдерами внешних услуг;
- нарушения договорных обязательств сторонними лицами;
- негативная информация о банке в прессе;
- несоответствие внутренних документов действующему законодательству;
- изменчивость и несогласованность требований надзорных и регулирующих органов, вышестоящих инстанций;

4.2.1.2. человеческий:

- массовое увольнение сотрудников банка или их потеря в результате несчастного случая;
- отсутствие (недостаточность) процедур планирования замещения должностей;
- несчастный случай на рабочем месте, повлёкший за собой гибель сотрудника (в том числе в результате суицида);
- некомпетентность, ошибка сотрудников банка;
- вандализм в отношении имущества банка;
- саботаж и (или) пикетирование и забастовки сотрудников банка;
- ошибки кадровой работы;
- ошибки в обеспечении безопасности информационных систем на стадиях жизненного цикла;
- нарушения сотрудниками банка организационных мер по обеспечению безопасности;

- выполнение вредоносных программ, использование информационных активов не по назначению;
- несанкционированный доступ к документам, автоматизированным системам и аппаратно-программному комплексу банка, инициативный шпионаж;
- кража ценностей, в том числе денежных средств, из помещения банка или во время их транспортировки;
- организованная преступность (создание преступных групп в структуре банка с целью извлечения незаконных доходов);
- запугивание и шантаж, социальный инжиниринг;
- гражданские беспорядки в регионе местонахождения банка;
- террористические акты или их угроза, а также взрывы криминогенного характера в помещении банка или в непосредственной близости от помещения банка или прилегающей к нему территории;
- локальные конфликты в регионе местонахождения банка;

4.2.1.3. техногенный:

- веерное отключение электроэнергии и (или) отказ систем электроснабжения, включая резервные источники питания;
- отказ функционирования средств вычислительной техники;
- атаки хакеров и крэкеров;
- компьютерные вирусы;
- отказ функционирования систем телекоммуникации;
- отказ функционирования систем программно-аппаратного комплекса по взаимодействию с платёжной системой ЦБ РФ;
- аварии систем жизнеобеспечения (прорыв канализации, трубопроводов горячей и холодной воды, отказ системы кондиционирования, отопления и др.);
- отравление химическими веществами;
- нарушения работы общественного транспорта;

4.2.1.4. природно-техногенный:

- пожар;
- падение искусственных и природных объектов с неба;

4.2.1.5. природный:

- экстремальные погодные условия (очень низкая или высокая температура воздуха, снежная буря, ураган);
- землетрясение;
- электромагнитные бури;
- эпидемии;
- наводнение;

4.2.1.6. страновые:

- некоторые запретительные акты государства (блокада, эмбарго, объявление карантина, ограничение перевозок на определённых направлениях, запрет некоторых торговых операций с отдельными странами вследствие применения международных санкций и т. д.);

4.2.1.7. финансовый:

- дефицит ликвидности банка, в том числе по причине потери деловой репутации;
- потеря (утрата) капитала;

4.2.1.8. прочие:

- другие обстоятельства, не отнесённые к вышеперечисленным, но имеющие место быть, в том числе согласно мнению всероссийского центра мониторинга и прогнозирования чрезвычайных ситуаций природного и техногенного характера «Антистихия» МЧС РФ.

4.3. Классификацией категорий (типов) нестандартных и чрезвычайных ситуаций в зависимости от нанесённого ущерба и продолжительности прерывания бизнес-процессов банка нестандартные и чрезвычайные ситуации подразделяются на НЧС, приносящие:

4.3.1. незначительный ущерб.

Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы), к непредвиденным не относятся. Возобновление операционной деятельности банка может быть осуществлено в короткое время без вызова специальных аварийных и технических служб. Ожидаемое время простоя - менее одного операционного дня. Ущерб может быть нанесён аппаратным средствам, программному обеспечению, механическому оборудованию, электрооборудованию и (или) зданию;

4.3.2. серьёзный ущерб.

НЧС, приводящие к выходу из строя отдельных компонентов системы банка (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа, – аварийные и технические службы вызываются для восстановления операционной деятельности банка в существующем помещении. Предполагаемое время простоя - от одного до пяти операционных дней. Нанесён серьёзный ущерб аппаратным средствам и (или) зданию;

4.3.3. катастрофа - обширный ущерб.

Восстановление потребует более пяти операционных дней. Здание может быть полностью разрушено. При катастрофе вызываются спасательные, аварийные и технические службы и все сотрудники банка, чтобы начать полное выполнение плана действий в случае возникновения нестандартных и чрезвычайных ситуаций.

4.4. В соответствии с постановлением № 304 чрезвычайные ситуации природного и техногенного характера подразделяются на:

4.4.1. чрезвычайные ситуации локального характера, в результате которых территория, на которой сложилась чрезвычайная ситуация и нарушены условия жизнедеятельности людей (далее – зона чрезвычайной ситуации), не выходит за пределы территории объекта, при этом количество людей, погибших или получивших ущерб здоровью (далее – количество пострадавших), составляет не более 10 человек либо размер ущерба окружающей природной среде и материальных потерь (далее – размер материального ущерба) составляет не более 100 тыс. руб.;

4.4.2. чрезвычайные ситуации муниципального характера, в результате которых зона чрезвычайной ситуации не выходит за пределы территории одного поселения или внутригородской территории города федерального значения, при этом количество пострадавших составляет не более 50 человек либо размер материального ущерба составляет не более 5 млн руб.,

а также данная чрезвычайная ситуация не может быть отнесена к чрезвычайной ситуации локального характера;

4.4.3. чрезвычайные ситуации межмуниципального характера, в результате которых зона чрезвычайной ситуации затрагивает территорию двух и более поселений, внутригородских территорий города федерального значения или межселенную территорию, при этом количество пострадавших составляет не более 50 человек либо размер материального ущерба составляет не более 5 млн руб.;

4.4.4. чрезвычайные ситуации регионального характера, в результате которых зона чрезвычайной ситуации не выходит за пределы территории одного субъекта РФ, при этом количество пострадавших составляет свыше 50 человек, но не более 500 человек либо размер материального ущерба составляет свыше 5 млн руб., но не более 500 млн руб.;

4.4.5. чрезвычайные ситуации межрегионального характера, в результате которых зона чрезвычайной ситуации затрагивает территорию двух и более субъектов РФ, при этом количество пострадавших составляет свыше 50 человек, но не более 500 человек либо размер материального ущерба составляет свыше 5 млн руб., но не более 500 млн руб.;

4.4.6. чрезвычайные ситуации федерального характера, в результате которых количество пострадавших составляет свыше 500 человек либо размер материального ущерба составляет свыше 500 млн руб.

4.5. По степени воздействия и размерам ущерба, наносимого банку, непредвиденные обстоятельства разделяются на следующие категории:

4.5.1. угрожающие - приводящие к неспособности банка полностью (частично) выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

4.5.2. серьёзные - приводящие к выходу из строя отдельных компонентов системы банка (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа;

4.5.3. ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки проникновения или несанкционированного доступа к ресурсам системы), к непредвиденным не относятся.

4.6. Ситуации, при возникновении которых не меняется порядок осуществления банковских операций:

- отключение (полное или частичное) электропитания (основного и резервного) менее чем на один час;
- нештатная работа аппаратно-программных компонентов автоматизированных рабочих мест (далее – АРМ) менее двух часов;
- повреждение телефонной сети;
- повреждение оптического кабеля (отсутствие доступа в сеть Интернет, SWIFT)

менее чем на два часа;

- сбой работы сервера баз данных менее чем на один час;
- сбой системного программного обеспечения (далее - ПО) менее чем на два часа;
- поломка аппаратных компонент сервера;
- прекращение доступа внешних пользователей к интернет-сайту банка;
- выход из строя (сбой) автоматизированной системы (или её модуля), разработанной сторонним разработчиком, менее чем на два часа;
- выход из строя автоматизированных прикладных модулей, разработанных управлением информационных технологий банка, менее чем на два часа;
- затопление в помещениях, занимаемых банком (незначительное, не влияющее на работу АРМ, произошедшее вне помещений, в которых находится серверное оборудование или обслуживание клиентов), возгорание (при возможности тушения возгорания в течение пяти минут силами сотрудников банка);
- выход из строя систем безопасности (охранной сигнализации, систем контроля доступа, системы видеонаблюдения).

5. Перечень ключевых бизнес-процессов по степени приоритетности

5.1. Для банка ключевыми являются следующие бизнес-процессы (по степени приоритетности):

- обслуживание клиентов;
- обработка информации и осуществление платежей;
- операции по привлечению и размещению ресурсов;
- обеспечение бесперебойной работы банка как расчётного центра платёжной системы «Мультисервисная платёжная система»;
- обеспечение безопасности, в том числе информационной;
- управление рисками;
- финансовый мониторинг и т. д.

6. Типовой перечень превентивных мер, выполнение которых в режиме повседневного функционирования банка необходимо для поддержания непрерывности деятельности

6.1. Перечень превентивных мер утверждается президентом банка, в его отсутствие – лицом, исполняющим его обязанности, или заместителем президента банка для головного офиса, или уполномоченными лицами (руководителями обособленных структурных подразделений банка) в соответствии с предоставленными полномочиями.

6.2. Перечень превентивных мер, выполнение которых в режиме повседневного функционирования банка необходимо для поддержания непрерывности деятельности, должен содержать процедуры и список мероприятий с указанием структурных подразделений банка или лиц, ответственных за их выполнение, наименование сторонних контрагентов (при наличии), учитывающих региональные, территориальные, технические и иные особенности каждого территориально обособленного внутреннего структурного подразделения банка.

6.3. Примерный перечень превентивных мер, выполнение которых в режиме повседневного функционирования банка необходимо для поддержания непрерывности деятельности головного офиса банка (см. табл. 1).

Таблица 1

№	Процедура (мероприятие)	Ответственное подразделение или контрагент	Описание или ссылка на контракт, договор, банковский документ	Сроки
1. В области охраны и поддержания непрерывности действия пропускного режима				
1.1	Охрана помещений банка, обеспечение защиты охраняемого имущества от противоправных посягательств, поддержание общественного порядка	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.2	Осуществление и поддержание непрерывности действия пропускного режима	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.3	Обеспечение допуска на охраняемую территорию	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.4	Осуществление мероприятий по предупреждению нарушений правил допуска на охраняемую территорию	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.5	Обеспечение сохранности материальных ценностей, защиты жизни и здоровья сотрудников	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.6	Обеспечение сохранности служебного автотранспорта, въезда во внутренний двор и выезда из него	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.7	Информирование руководства банка о выявленных фактах или попытках хищения, повреждения, уничтожения имущества и иных материальных ценностей	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.8	Обеспечение охраны места происшествия до момента прибытия сотрудников МВД	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.9	Обеспечение обновления информации о телефонах служб	Служба безопасности	Должностные инструкции, договор об оказании	Постоянно

	быстрого реагирования		охранных услуг	
1.10	Взаимодействие с правоохранительными, государственными и коммерческими структурами в интересах обеспечения безопасности банка	Служба безопасности	Должностные инструкции, договор об оказании охранных услуг	Постоянно
1.11	Наблюдение за состоянием помещений, проведение ремонта, обеспечение работоспособности коммуникаций	Организация-арендодатель, управление делами, отдел материально-технического обеспечения управления делами (ОМТО УД)	Договор аренды помещений, договоры на обслуживание соответствующих систем	Постоянно
2. В области энергоснабжения				
2.1	Обеспечение непрерывности энергоснабжения	ОМТО УД	Договор аренды помещений, договоры на обслуживание соответствующих систем, должностные инструкции сотрудников соответствующего подразделения	Постоянно
2.2	Обеспечение дублирования технических средств	ОМТО УД	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
3. В области охраны здоровья				
3.1	Осуществление кондиционирования воздуха	ОМТО УД	Договор аренды помещений, договоры на обслуживание соответствующих систем	Постоянно
4. В области противопожарной охраны				
4.1	Установка, обслуживание и обеспечение функционирования в исправном состоянии пожарных систем, пожарной и тревожной сигнализации, специальных средств, средств пожаротушения в арендуемых	ОМТО УД	Договор аренды помещений, договоры на обслуживание соответствующих систем	Постоянно

	помещениях банка			
4.2	Установка, обслуживание и обеспечение функционирования в исправном состоянии пожарных систем, пожарной и тревожной сигнализации, специальных средств, средств пожаротушения в архиве и хранилище банка	ОМТО УД	Договоры на обслуживание соответствующих систем	Постоянно
4.3	Мероприятия по проверке работоспособности обеспечения надлежащего функционирования систем охранно-пожарной сигнализации (датчиков оповещения при появлении дыма) в помещениях, а также действий сотрудников банка при ЧС	ОМТО УД	Согласно плану мероприятий	Регулярно, но не менее трёх раз в год
5. В области противорадиационной защиты				
5.1	Выделение и оборудование комнаты для работы с денежными знаками с радиационным загрязнением	ОМТО УД, расчётный центр	Требования Банка России: • Инструкция Банка России от 04.12.07 № 131-И «О порядке выявления, временного хранения, гашения и уничтожения денежных знаков с радиоактивным загрязнением»; • письмо Банка России от 26.12.11 № 29-15/8294 «О необходимости осуществления радиационного контроля денежной наличности, поступающей в кредитные организации»; • распорядительный документ по банку	Постоянно

			(распоряжение); • должностные инструкции сотрудников соответствующего подразделения	
5.2	Работа с денежными знаками с радиационным загрязнением производится с использованием средств индивидуальной защиты и специальных приборов	ОМТО УД, начальник расчётного центра	Требования Банка России: • Инструкция Банка России от 04.12.07 № 131-И «О порядке выявления временного хранения, гашения и уничтожения денежных знаков с радиоактивным загрязнением»; • письмо Банка России от 26.12.11 № 29-15/8294 «О необходимости осуществления радиационного контроля денежной наличности, поступающей в кредитные организации»; • распорядительный документ по банку (распоряжение); • должностные инструкции сотрудников соответствующего подразделения	Ежедневно
6. В области правового обеспечения				
6.1	Анализ условий договоров страхования, обеспечение правовой экспертизы документов, предоставленных страховыми компаниями для заключения всех видов договоров страхования	Управление правового обеспечения (УПО)	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно

6.2	Проверка наличия необходимых документов, их соответствия требованиям законодательства, полномочиям лиц, заключающих сделку и подписывающих договор страхования, реквизитов для уплаты страховых взносов и получения возмещения	УПО	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно
6.3	Анализ причин возникшего в случае непредвиденных обстоятельств ущерба, расчёт ущерба, сбор необходимых документов для дальнейшего направления претензий виновнику происшествия, в правоохранительные органы, а также в страховую компанию	УПО, финансово-аналитическое управление (ФАУ), управление учёта и налоговой отчётности (УУНО) - первый заместитель главного бухгалтера	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно
6.4	Направление претензий виновнику происшествия и запроса в страховую компанию на выплату страховой суммы за причинённый банку ущерб	Управление правового обеспечения	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно
6.5	Получение и правовой анализ всех заявлений об ущербе	УПО, ФАУ, УУНО - первый заместитель главного бухгалтера	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно
6.6	Обеспечение представления интересов банка в государственных органах, в том числе в суде, по вопросам взыскания ущерба с виновных лиц	УПО	Договоры страхования, требования законодательства по обязательному и добровольному страхованию, должностные инструкции сотрудников соответствующего подразделения	Постоянно

6.7	Взаимодействие со службой судебных приставов (после получения решения суда и исполнительного листа о взыскании ущерба или страховой суммы со страховой компании) в целях взыскания денежных средств, необходимых для восстановления деятельности банка	УПО, служба безопасности	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
6.8	Обеспечение сохранности правоустанавливающих, учредительных и регистрационных документов банка, протоколов заседания наблюдательного совета и общего собрания акционеров банка, а также комитета по проблемным активам (КПА)	УПО	Должностные инструкции сотрудников соответствующего подразделения, внутренние документы банка	Постоянно
6.9	Копирование и отдельное хранение наиболее важных документов (распорядительных и внутренних нормативных документов), хранение наиболее важных документов в несгораемом сейфе	Структурные подразделения банка	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
7. В области функционирования систем телефонии и средств связи				
7.1	Обеспечение непрерывности функционирования сетей телефонии и связи, использование мобильной связи (резервная линия связи), приобретённые мобильный телефон и сим-карта хранятся в ОМТО УД	ОМТО УД, управление информационных технологий (УИТ)	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
7.2	Обеспечение обновления информации о сетях связи, её поставщиках и провайдерах	УИТ	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
7.3	Дублирование технических средств, в том числе средств связи	УИТ, ОМТО УД, отдел	Должностные инструкции сотрудников соответствующего подразделения,	Постоянно

		информационной безопасности службы безопасности (ОИБ СБ)	политики в области ИТ и ИБ	
8. В области информационных технологий				
8.1	Оценка степени критичности автоматизированных банковских систем, аппаратно-программного комплекса и других существенно значимых данных в компьютерной сети банка	УИТ	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
8.2	Хранение копий всех конфигураций аппаратных средств банка	УИТ	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
8.3.	Обеспечение мер по хранению данных списков вне основного производственного помещения	Отдел информационной безопасности службы безопасности (ОИБ СБ)		Постоянно
8.4	Поддержание аппаратных средств и другого оборудования АБС, включая резервное, в рабочем состоянии и периодическая их проверка	УИТ, ОИБ СБ	Частная политика резервного копирования и восстановления данных	В соответствии с графиком
8.5	Выявление критически важных систем и подготовка детальных планов восстановления	УИТ, ОИБ СБ		Раз в полугодие
8.6	Реализация процедур резервного копирования данных на магнитные носители, хранимые вне серверных комнат	УИТ	Частная политика резервного копирования и восстановления данных	Постоянно
8.7	Обеспечение полноты мер по хранению резервной копии базы данных вне основного производственного помещения; обеспечение возможности восстановления с использованием резервных копий, хранящихся вне основного производственного помещения	УИТ, ОИБ СБ	Частная политика резервного копирования и восстановления данных	Постоянно

8.8	Дублирование технических средств, в том числе средств связи, резервных каналов связи	ОМТО УД, УИТ, отдел расчётных систем и банковских телекоммуникаций	Должностные инструкции сотрудников соответствующего подразделения	Постоянно
9. В области информационной безопасности				
9.1	Мероприятия осуществляются в соответствии с принятыми политиками в области обеспечения информационной безопасности	ОИБ СБ, УИТ, структурные подразделения банка	Законы, постановления Правительства РФ, документы ЦБ РФ, регулирующие данное направление деятельности, документы регуляторов, а также внутренние документы банка по ИБ	Постоянно
10. В области кадровой политики				
10.1	Планирование и подбор квалифицированного персонала, сотрудников	Отдел по работе с персоналом управления делами	Должностные инструкции сотрудников	Постоянно
10.2	Осуществление программы «Знай своего служащего» – проверка новых сотрудников службой безопасности банка	Служба безопасности, руководители структурных подразделений банка, отдел по работе с персоналом управления делами	Должностные инструкции сотрудников	При приёме на работу
10.3	Планирование и осуществление обучения сотрудников, проведение аттестации	Отдел по работе с персоналом управления делами	Внутренние документы банка и должностные инструкции сотрудников	На регулярной основе
11. В области экономической безопасности и финансового мониторинга				
11.1	Мониторинг и оценка вероятности неисполнения контрагентами своих обязательств перед банком	Руководители соответствующих подразделений, ФАУ, служба безопасности	Должностные инструкции сотрудников, внутренние документы банка (регламенты службы безопасности, положения о порядке формирования резервов на возможные потери и возможные потери по ссудам, регламент осуществления работы по внутрихозяйственной	Ежедневно

			деятельности)	
11.2	Мониторинг и осуществление внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма (ПОД/ФТ)	Ответственный сотрудник по ПОД/ФТ, сотрудники банка	ПВК по ПОД/ФТ, внутренние документы банка, должностные инструкции, положения о внутренних структурных подразделениях	Ежедневно
12. В области мониторинга и оценки банковских типовых и неспецифических рисков				
12.1	Мониторинг и оценка операционных, рыночных, кредитных, страновых рисков, рисков потери деловой репутации и правового риска, совокупного риска банка	ФАУ, служба управления рисками (СУР)	Положение о службе управления рисками, внутренние регламенты	В сроки, установленные внутрибанковским регламентом
12.2	Мониторинг и оценка показателей и нормативов ликвидности банка	ФАУ, СУР, казначейство	Положение о службе управления рисками, внутренние регламенты	В сроки, установленные внутрибанковским регламентом
12.3	Анализ и оценка влияния непредвиденных обстоятельств и понесённого в результате их воздействия ущерба на показатели деятельности банка	ФАУ, СУР, СВК	Положение о службе управления рисками, внутренние регламенты	В сроки, установленные внутрибанковским регламентом
13. В области поддержания ликвидности и платёжеспособности				
13.1	Мониторинг ликвидности и платёжной позиции банка	ФАУ, СУР, СВК	Положение по управлению и контролю за ликвидностью и риском ликвидности	Постоянно

13.2	Обеспечение мер по поддержанию ликвидности банка	ФАУ, СУР, СВК	Положение по управлению и контролю за ликвидностью и риском ликвидности	Постоянно
13.3	Заключение договоров с банками и компаниями-контрагентами в соответствии с установленными (устанавливаемыми) лимитами	ФАУ, СУР, УПО	Положение по управлению и контролю за ликвидностью и риском ликвидности, положение о кредитном комитете	Постоянно
14. В области обучения				
14.1	Ознакомление с планом, обеспечение непрерывности деятельности за счёт их обучения	Руководители структурных подразделений банка	Программа изучения и проведения проверок	Не реже одного раза в два года
14.2	Проведение учений, тестирование плана ОНиВД	Руководство банка, СВК	Порядок тестирования плана по обеспечению непрерывности деятельности и (или) восстановления деятельности в случае возникновения нестандартных и чрезвычайных ситуаций	В соответствии с графиком
15. В области обеспечения и организации мероприятий по гражданской обороне (ГО) и чрезвычайным ситуациям (ЧС)				
15.1	Обучение с программой курсового обучения сотрудников в области гражданской обороны и чрезвычайным ситуациям в банке	Уполномоченные по делам ГО и ЧС, ОИБ СБ	Программа курсового обучения сотрудников	Ежегодно, в объёме не менее 16 часов
15.2	Проведение вводного инструктажа по гражданской обороне и предотвращению чрезвычайных ситуаций со всеми лицами, принимаемыми на работу в банк	Уполномоченные по делам ГО и ЧС, ОИБ СБ	Программа вводного инструктажа	При приёме на работу

6.4. Документы, подлежащие копированию и отдельному хранению (см. табл. 2).

Таблица 2

Вид документа	Место хранения	Место хранения резервной копии	Ответственный сотрудник
Уставные документы	Управление правового обеспечения (УПО)	Сейф резервного помещения	Начальник УПО
Лицензии	Управление правового обеспечения (УПО)	Сейф резервного помещения	Начальник УПО
Договоры МБК, генеральное соглашение с Банком России	Казначейство	Сейф резервного помещения	Начальник казначейства
Документы по эмиссиям	Управление правового обеспечения (УПО)	Сейф резервного помещения	Начальник УПО
Кредитные договоры, договоры обеспечения, соглашения о предоставлении банковских гарантий	Кредитно-финансовое управление (КФУ)	Сейф резервного помещения	Начальник КФУ
Кредитные договоры овердрафт к банковским картам	Центр электронных услуг и обслуживания физических лиц (ЦЭУ)	Сейф резервного помещения	Начальник ЦЭУ

В случае утраты оригиналов документов они восстанавливаются на основе заверенных копий.

6.5. Руководители обособленных структурных подразделений банка обеспечивают разработку и утверждение перечня превентивных мер, выполнение которых в режиме повседневного их функционирования необходимо для поддержания непрерывности деятельности.

Кредитно-финансовый отдел обеспечивает копирование и отдельное хранение кредитных договоров, договоров обеспечения в сейфе резервного помещения.

7. Основные этапы и порядок реализации плана ОНиВД

7.1. Уведомление о нестандартных и чрезвычайных ситуациях, активация плана ОНиВД. Основные задачи, решаемые на данном этапе, – своевременная идентификация наступления нестандартной и (или) чрезвычайной ситуации, обнаружение, предварительная оценка нанесённого ущерба и принятие решения о необходимости активации плана ОНиВД.

7.2. Восстановление работоспособности банка. Основные задачи – восстановление

функционирования банка по временной схеме (с использованием резервных средств и помещений), проведение комплекса работ по полному восстановлению деятельности банка в обычных объёмах деятельности.

7.3. Возврат к нормальному функционированию системы, деактивация плана ОНиВД. Основные задачи – полное восстановление нормальной работы банка и деактивация плана ОНиВД, возврат к нормальному функционированию.

7.4. Порядок принятия решения о переводе деятельности банка в режим, предусмотренный планом ОНиВД.

7.4.1. Ответственным за взаимодействие и информационный обмен в случае наступления негативных непредвиденных обстоятельств, которые могут повлечь нарушение деятельности банка, является координатор – начальник службы безопасности банка.

7.4.2. Решение о переводе деятельности банка в чрезвычайный режим в случае возникновения нестандартных и чрезвычайных ситуаций (далее – чрезвычайный режим) принимается президентом банка или лицом, исполняющим его обязанности на основе сообщения о наступлении непредвиденных обстоятельств и подтверждения информации координатором – начальником службы безопасности.

7.4.3. Приказом президента банка или лица, исполняющего его обязанности, создаётся группа управления в чрезвычайных ситуациях с определением персонального состава ГУЧС головного офиса банка.

7.4.4. Персональный состав ГУЧС филиалов банка назначается приказом руководителя (директора) филиала по согласованию с президентом банка или лица, исполняющего его обязанности. Управление в чрезвычайных ситуациях в территориально удалённых структурных подразделениях банка (дополнительных офисах, кредитно-кассовых офисах и др.) возлагается на руководителя структурного подразделения банка с учётом требования пункта 7.4.7 настоящего плана.

7.4.5. В состав группы управления в чрезвычайных ситуациях входят:

- президент банка и (или) его первый заместитель;
- начальник службы безопасности (координатор);
- начальник службы внутреннего контроля;
- начальник службы внутреннего аудита;
- главный бухгалтер или его заместитель;
- управляющий делами;
- начальник управления информационных технологий (УИТ);
- начальник управления правового обеспечения (УПО);
- начальник кредитно-финансового управления (КФУ);
- начальник казначейства;
- начальник расчётного центра;
- начальник центра электронных услуг и обслуживания физических лиц.

7.4.6. В случае возникновения нестандартных и чрезвычайных ситуаций и перевода банка в чрезвычайный режим деятельности президент банка или лицо, исполняющее его обязанности, вправе определить иной первичный персональный состав ГУЧС и ориентировочный срок действия

чрезвычайного режима.

7.4.7. Филиалы, дополнительные офисы, операционные кассы вне кассового узла, кредитно-кассовые и операционные офисы, иные внутренние структурные подразделения банка также руководствуются действиями ГУЧС.

7.4.8. Информирование всех сотрудников банка о наступлении чрезвычайного режима организует управляющий делами.

7.4.9. Информирование заинтересованных лиц осуществляется в соответствии с приложением 3.

7.4.10. Выработку коммуникативных методов чрезвычайной группы организует координатор.

7.4.11. Список и контактные телефоны ответственных сотрудников дежурных и оперативных служб приведены в списке телефонов сотрудников, на регулярной основе обновляемом и размещаемом уполномоченным сотрудником банка в сети банка в папке общего доступа (и на бумажном носителе у управляющего делами).

7.5. Порядок управления банком в чрезвычайном режиме

7.5.1. ГУЧС создаётся и начинает функционировать с момента объявления чрезвычайного режима. ГУЧС прекращает свою деятельность только по распоряжению президента банка или лица, исполняющего его обязанности. Все сотрудники банка после получения сообщения о наступлении чрезвычайного режима обязаны беспрекословно выполнять указания президента банка или лица, исполняющего его обязанности, координатора, членов ГУЧС, непосредственных руководителей в указанной последовательности. ГУЧС в течение 90 минут вырабатывает план первичных мероприятий, предлагает распределение полномочий и компетенций на период чрезвычайного режима и организует при необходимости первичные спасательные работы. В плане первичных мероприятий определяются и конкретизируются основные работы по обеспечению непрерывности, восстановления деятельности банка, определяются методы реализации модулей плана ОНиВД.

План первичных мероприятий согласовывается с президентом банка или лицом, исполняющим его обязанности, после чего ГУЧС приступает к немедленной реализации плана. При невозможности восстановления критически важных банковских процессов в течение 36 часов ГУЧС по истечении четырёх часов с момента наступления чрезвычайного режима вырабатывает комплексный план по восстановлению деятельности банка:

- определяет степень влияния непредвиденных обстоятельств на деятельность банка;
- составляет перечень потерь;
- оценивает размер нанесённого ущерба.

7.6. Функции ГУЧС:

- координация работ по обеспечению непрерывности и (или) восстановления деятельности банка, принятие решений о реализации модулей плана ОНиВД;
- информирование заинтересованных лиц о ходе восстановления деятельности банка и (или) мерах, принятых для обеспечения её непрерывности;

- взаимодействие с Банком России в целях координации совместных действий по обеспечению своевременного проведения расчётов по поручениям клиентов и по обязательствам банка, а также с другими заинтересованными лицами по вопросам обеспечения непрерывности и (или) восстановления деятельности;
- взаимодействие с правоохранительными органами, аварийными и специализированными службами (в том числе с органами внутренних дел, пожарной охраной, аварийно-спасательными службами, учреждениями здравоохранения, органами, осуществляющими государственный санитарно-эпидемиологический надзор);
- определение факторов, вызвавших кризисную ситуацию (внешние или внутренние), а также признаков, свидетельствующих о возникновении кризисной ситуации;
- определение стратегических действий и необходимости масштаба их введения;
- разработка и представление на утверждение наблюдательного совета плана мероприятий, назначение ответственных за исполнение мероприятий, координация взаимодействия подразделений-исполнителей, контроль исполнения мероприятий;
- информирование членов правления банка и наблюдательного совета о результатах мероприятий и изменениях контрольных показателей (динамике клиентских средств, возможностях приобретения срочных депозитов и межбанковских средств по текущей рыночной стоимости, репутации банка и т. д.);
- определение момента выхода из кризиса и плана возврата к обычному режиму работы, анализ произошедших событий, выводы об эффективности предпринятых мер и о том, насколько можно избежать повторения кризисной ситуации;
- принятие решения по вопросам обеспечения общественности необходимой информацией (либо ограничениях на распространение сведений определённого характера).

В целях реализации плана ОНиВД и сохранения уровня управления банком в случае возникновения нестандартных и чрезвычайных ситуаций ГУЧС возможна передача полномочий по оперативному руководству деятельностью банка в следующем объёме:

- утверждение предельных значений коэффициентов избытка (дефицита) ликвидности;
- реструктуризация активов и обязательств по срокам;
- определение источников и лимитов для привлечения ресурсов по срокам;
- определение признаков, свидетельствующих о возникновении кризиса ликвидности;
- составление текущего и краткосрочного прогноза ликвидности;
- контроль соблюдения установленных лимитов по суммам кредитов по срокам их востребования;
- анализ состояния ликвидности с использованием сценариев негативного для банка развития событий;
- выработка рекомендаций по окончанию срока сделок по проводимым активным операциям;
- выработка рекомендаций при заключении сделок по проводимым пассивным операциям;
- принятие мер по досрочному возврату межбанковских кредитов, пересмотр сроков выдаваемых межбанковских кредитов;
- инициация изменения процентных ставок и тарифов;
- предложение и оценка новых продуктов по привлечению депозитных средств;
- контроль за соблюдением установленных предельных значений коэффициентов избытка (дефицита) ликвидности;
- инициация внесения изменений в показатели, используемые для оценки уровня

ликвидности, выработка рекомендаций по восстановлению ликвидности;

- разработка и предоставление на утверждение правлению банка и наблюдательному совету банка в пределах их полномочий мероприятий по преодолению кризиса ликвидности и контроль их исполнения;
- определение момента выхода из кризисной ситуации и возврата к обычному режиму работы.

7.7. Порядок осуществления внутренних банковских процессов в чрезвычайном режиме

Уровень осуществления банковских процессов при наступлении чрезвычайного режима зависит от масштабов и характера повреждений и определяется банком в зависимости от степени важности процесса следующим образом (см. табл. 3).

Таблица 3

№	Процесс	Уровень осуществления	Комментарии
1	Проведение платежей клиентов	1	В соответствии с законодательством РФ и заключёнными договорами
2	Проведение таможенных платежей клиентов в рамках работы расчётного центра	1	В соответствии с законодательством РФ и правилами платёжной системы «Мультисервисная платёжная система»
3	Кассовое обслуживание	1	В соответствии с законодательством РФ и заключёнными договорами
4	Мониторинг операций и отправка сообщений в целях ПОД/ФТ	1	В соответствии с законодательством РФ
5	Исполнение обязательств по полученным кредитам (депозитам)	1	В соответствии с законодательством РФ
6	Операции на рынке ценных бумаг (купля-продажа ценных бумаг)	1	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
7	Принятие и рассмотрение кредитных заявок, заявок на предоставление гарантий и поручительств	2/3	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
8	Оценка кредитных рисков по выданным ссудам	3	Производится в соответствии с внутренними регламентами банка раз в месяц на отчётную дату
9	Открытие счетов клиентам	3	В зависимости от доступности ресурсов на осуществление

1	Инкассация	1	В соответствии с заключёнными договорами
1	Купля-продажа иностранной валюты (для закрытия позиции банка)	1	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
1	Купля-продажа иностранной валюты (по поручению клиентов)	2/3	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
1	Осуществление переводов без открытия счёта	2/3	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
1	Бухгалтерский учёт операций банка	1	В соответствии с законодательством РФ
1	Проведение сделок РЕПО	1	В зависимости от доступности ресурсов для осуществления и состояния ликвидности банка; решение о приемлемом уровне осуществления принимает руководитель ГУЧС
1	Выполнение функций агента валютного контроля	1	В соответствии с законодательством РФ и принятыми на себя обязательствами
1	Осуществление внутреннего контроля	1	В соответствии с законодательством РФ

8. Хранение и актуализация плана ОНиВД

8.1. План хранится в бумажном виде:

- у руководителей структурных подразделений банка;
- руководителя службы безопасности банка.

8.2. Электронная копия плана хранится в корпоративном хранилище документов.

8.3. Внесение изменений в контактную информацию производится в срок не позднее двух

рабочих дней после её изменения. Сбор и корректировку информации осуществляет служба внутреннего контроля банка. За своевременное и полное представление контактной информации несут ответственность руководители структурных подразделений банка.

8.4. Контроль за эффективностью и актуальностью плана осуществляет служба внутреннего контроля банка.

9. Порядок актуализации плана ОНиВД

9.1. План ОНиВД рекомендуется пересматривать не реже одного раза в два года с целью обеспечения его соответствия организационной структуре, характеру и масштабам деятельности банка, утверждённой стратегии развития деятельности банка, условиям мест нахождения банка (обособленных структурных подразделений банка), а также в целях устранения недостатков, выявленных в ходе проверок (тестирования) плана ОНиВД, и учёта вновь выявленных факторов, которые могут привести к нарушению повседневного функционирования банка.

9.2. При обновлении плана ОНиВД или приложений к нему уточнению подлежат:

- перечень решаемых задач, конфигурации технических и программных средств АБС, приводящих к изменению технологии обработки информации;
- состав, обязанности и полномочия пользователей АБС;
- состав, обязанности и полномочия руководителей групп по поддержанию непрерывности деятельности и ликвидации последствий непредвиденных обстоятельств;
- вспомогательная информация (схемы, адреса, списки поставщиков и т. д.);
- потребность в технических средствах и программном обеспечении для основных и резервных помещений;
- список необходимых внешних ресурсов, включая технические средства, программное обеспечение, средства связи, данные, документы, офисное оборудование, документацию и персонал.

9.3. В целях оценки работоспособности и эффективности плана ОНиВД используются обсуждения его разделов с сотрудниками банка и учебные чрезвычайные ситуации.

9.4. Каждое непредвиденное обстоятельство (чрезвычайная ситуация) анализируется ГУЧС в соответствии с политикой информационной безопасности и оценивается по следующим критериям:

- случайность или преднамеренность возникновения непредвиденного обстоятельства (чрезвычайной ситуации);
- учёт возможности непредвиденного обстоятельства (чрезвычайной ситуации) планом ОНиВД;
- возможность прогнозирования возникновения непредвиденного обстоятельства (чрезвычайной ситуации) данного вида;
- обусловленность возникновения непредвиденного обстоятельства (чрезвычайной ситуации) слабостью средств защиты и регистрации;
- соотношение ущерба от непредвиденного обстоятельства (чрезвычайной ситуации) с установленным уровнем;
- наличие невосполнимого ущерба и его размера;

- возможность точно установить виновника;
- возможность точно установить причину чрезвычайной ситуации;
- необходимость пересмотра плана ОНиВД.

9.5. По результатам анализа, произведённого в соответствии с подпунктом 9.4, ГУЧС вырабатываются предложения по изменению полномочий сотрудников банка, атрибутов доступа к ресурсам, созданию дополнительных резервов, изменению конфигурации системы или параметров настройки средств защиты и т. д.

9.6. Если причиной чрезвычайной ситуации явились недостаточные меры защиты и контроля, то такая ситуация является основанием для пересмотра или коррекции политики информационной безопасности и плана ОНиВД.

9.7. Вносимые в план ОНиВД изменения не должны противоречить другим его статьям и предварительно проверяются на корректность, полноту и выполнимость.

9.8. Обновлённый план ОНиВД размещается на сетевом ресурсе банка в открытом для всех сотрудников доступе с уведомлением об этом каждого сотрудника путём рассылки по банку.

9.9. Ответственность за своевременный пересмотр, обновление плана ОНиВД несут служба внутреннего контроля банка и служба безопасности банка.

10. Порядок проверки (тестирования) плана ОНиВД

10.1. С целью определения возможности выполнения плана ОНиВД в случае возникновения нестандартных и чрезвычайных ситуаций предусматривается проведение проверок (тестирования) плана ОНиВД с периодичностью не реже одного раза в два года. При проверке (тестировании) отдельных модулей плана ОНиВД (приложений) производится проверка (тестирование) каждого из них с соблюдением периодичности, установленной для плана ОНиВД в целом.

10.2. Для обеспечения постоянной готовности сотрудников банка к действиям на случай нестандартных и чрезвычайных ситуаций организовывается изучение плана ОНиВД на регулярной основе всеми сотрудниками банка в соответствии со специально разработанной для этих целей программой, включающей проведение учений. Учения планируются таким образом, чтобы оценить реальное время, необходимое для выполнения каждого модуля плана ОНиВД, и степень подготовленности сотрудников банка к работе в чрезвычайном режиме.

При подготовке проверки (тестирования) плана ОНиВД в форме учений:

- учитываются возможные проблемы, в том числе психологического характера, связанные с необычностью ситуации;
- ставятся перед участниками учений цели по выявлению недостатков плана ОНиВД для мотивации их на его совершенствование.

Решение о проведении проверки (тестирования) плана ОНиВД оформляется в соответствии с установленным банком порядком. При этом определяются:

- программа, форма и сроки проведения проверки (тестирования) плана ОНиВД;
- перечень подразделений и сотрудников банка, участвующих в проверке (тестировании) плана ОНиВД;

- перечень проверяемых (тестируемых) модулей плана ОНиВД (приложений);
- перечень ресурсов, предполагаемых для использования при проверке (тестировании) плана ОНиВД;
- состав и обязанности группы наблюдателей (контролёров);
- сроки и порядок оформления результатов проверки (тестирования) плана ОНиВД.

Проверка (тестирование) плана ОНиВД проводится по заранее разработанной и утверждённой президентом банка программе, предусматривающей вводные данные (описание сценариев возникновения непредвиденных обстоятельств и связанных с ними факторов нарушения режима повседневного функционирования), подробное описание действий сотрудников банка в соответствии с проверяемым (тестируемым) планом ОНиВД или модулем плана ОНиВД, требованиями по срокам завершения промежуточных этапов выполнения плана ОНиВД.

Для проведения проверки (тестирования) плана ОНиВД определяется группа наблюдателей (контролёров), на которую возложен контроль выполнения предусмотренных планом ОНиВД мероприятий, составление протокола проверки (тестирования) и отчёта о проведении проверки (тестирования) плана ОНиВД.

Для работы в составе группы наблюдателей (контролёров) привлекаются сотрудники банка (обособленных структурных подразделений банка), ответственные за разработку плана ОНиВД, сотрудники службы безопасности, управления делами, представители службы внутреннего аудита и, при необходимости, сотрудники других структурных подразделений банка, независимые специалисты из организаций, специализирующихся на оказании консультационных услуг в сфере обеспечения непрерывности деятельности и информационной безопасности кредитных организаций.

10.3. Цели тестирования плана ОНиВД:

- проверка актуальности и работоспособности плана ОНиВД и обеспечения восстановления сервисов в указанные сроки;
- проверка готовности сотрудников банка и руководителей банка к работе в условиях нестандартных и чрезвычайных ситуаций;
- закрепление и совершенствование навыков, приобретённых в процессе обучения;
- выявление необходимости пересмотра и (или) внесения изменений в план ОНиВД.

10.4. Основным методом тестирования плана ОНиВД банка является имитационное моделирование – презентация и рассмотрение гипотетического сценария развития событий с руководителями ответственных структурных подразделений банка, а также практическая отработка отдельных мероприятий, предусмотренных планом ОНиВД.

10.5. Группа тестирования плана ОНиВД разрабатывает программу тестирования плана ОНиВД, которая включает сценарии учений и испытаний, распределение обязанностей между представителями структурных подразделений банка в части проведения учений и испытаний.

10.6. В программу тестирования включаются следующие разделы:

- описание сценариев возникновения нестандартных и чрезвычайных ситуаций и связанных с ними факторов нарушения режима повседневного функционирования;
- подробное описание всех этапов теста с указанием их целей, задач и порядка проведения;

- участники тестирования, распределение ролей и обязанностей между участниками тестирования;
- объекты тестирования;
- требования по срокам завершения промежуточных этапов выполнения плана ОНиВД.

10.7. По результатам проверки (тестирования) плана ОНиВД группа наблюдателей оформляет протокол проверки (тестирования).

В протоколе указываются:

- список наблюдателей (контролёров), присутствующих при проведении проверки (тестирования), с указанием лица, ответственного за ведение протокола;
- перечень всех процедур, выполняемых в рамках тестируемых модулей плана ОНиВД, с отметками о соответствии результатов их выполнения плану ОНиВД;
- время, затраченное на завершение промежуточных этапов и реализацию проверяемых (тестируемых) модулей плана ОНиВД;
- описание выявленных недостатков плана ОНиВД или подготовки сотрудников - участников проверки.

Протокол проверки (тестирования) плана ОНиВД согласовывается с руководителями задействованных в проверке (тестировании) плана ОНиВД структурных подразделений банка.

Отчёт по итогам проведения проверки (тестирования) плана ОНиВД составляется на основании согласованного протокола проверки (тестирования) плана ОНиВД. В отчёт включается анализ результатов проверки (тестирования) плана ОНиВД, предложения по устранению выявленных недостатков и совершенствованию плана ОНиВД.

10.8. По результатам тестирования проводится актуализация плана ОНиВД.

10.9. Контроль за выполнением требований порядка проверки (тестирования) плана ОНиВД возлагается на службу внутреннего контроля и службу безопасности банка.

11. Роль службы внутреннего контроля в управлении непрерывностью деятельности банка

11.1. Управление непрерывностью бизнеса является составной частью политики управления рисками банка. Сотрудники СВК рассматривают каждый модуль плана ОНиВД и систему управления непрерывностью деятельности банка в целом. Периодичность и глубина рассмотрения определяются значимостью для банка отдельных бизнес-процессов (по результатам оценки связанных с ними рисков) и вероятностью их нарушений.

11.2. Служба внутреннего контроля банка прежде всего контролирует решение таких вопросов, как:

- своевременность обновления и пересмотра планов ОНиВД и сопутствующей им документации;
- доведение регламентов по непрерывности деятельности банка до сведения всех заинтересованных лиц (руководства банка, ответственных структурных подразделений или отдельных сотрудников банка);
- покрытие планами ОНиВД и сопутствующими им документами всех существенных направлений деятельности банка;

- адекватность процедур по восстановлению непрерывности деятельности возникающим рискам и последствиям чрезвычайной ситуации;
- установление структурных подразделений (сотрудников) банка, ответственных за управление и принятие решений в чрезвычайных обстоятельствах;
- обеспечение взаимодействия со всеми необходимыми лицами и структурами (обеспечение каналов обмена информацией с внешней средой).

11.3. Помимо проведения контрольных мероприятий сотрудники СВК участвуют в самом процессе управления непрерывностью, начиная с консультирования структурных подразделений банка в разработке планов ОНиВД и заканчивая участием в мероприятиях по восстановлению непрерывности деятельности банка после возникновения нестандартных и чрезвычайных ситуаций.

11.4. При разработке планов ОНиВД сотрудники СВК вовлекаются в определение приоритетов и очерёдности действий в рамках плана ОНиВД по итогам оценки изменений внешней и внутренней среды, а также для адекватного измерения рисков по основным бизнес-процессам банка. Кроме того, сотрудники СВК проводят анализ разрабатываемых обособленными структурными подразделениями банка планов ОНиВД на предмет соответствия плану ОНиВД в целом и устанавливаемым им качественным критериям.

11.5. СВК осуществляет на регулярной основе мониторинг эффективности и качества принимаемых мер по налаживанию нормальной жизнедеятельности банка, особенно тех областей, которые подвержены наибольшим рискам в силу своей специфики и (или) наиболее пострадали от чрезвычайных обстоятельств. После завершения восстановительного периода СВК проводит специальную проверку качества восстановления бизнес-процессов, анализирует извлечённые из ситуации уроки. Итогом подобной проверки может стать формирование плана мероприятий по изменению документов, ресурсов (материальных и нематериальных), методик и систем управления, направленных на предотвращение чрезвычайной ситуации или уменьшение степени её влияния на деятельность банка в будущем.

12. Обучение сотрудников банка действиям по поддержанию непрерывности деятельности банка

12.1. В целях обеспечения непрерывности деятельности банка организуется изучение плана ОНиВД при приёме на работу, а также на регулярной основе.

12.2. Обучение сотрудников банка действиям, обеспечивающим непрерывность деятельности банка в соответствии с планом ОНиВД, осуществляется ответственными структурными подразделениями банка при контроле службы безопасности банка и службы внутреннего контроля.

12.3. Результаты обучения заносятся в личную карточку сотрудника банка.

13. Порядок действий сотрудников (персонала) банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций

13.1. Порядок действий сотрудников (персонала) головного офиса банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций, определён приложениями к настоящему плану с учётом особенности и причин возникновения нестандартных и чрезвычайных ситуаций.

13.2. Порядок действий сотрудников (персонала) обособленных структурных подразделений банка и перечень мероприятий, которые должны быть выполнены в момент возникновения и после возникновения нестандартных и чрезвычайных ситуаций, определяются приложениями к планам ОНиВД, разработанными обособленными структурными подразделениями банка в соответствии с принципами, заложенными в настоящем плане ОНиВД, и с учётом региональных (территориальный, природных, иных) особенностей и причин возникновения нестандартных и чрезвычайных ситуаций.

Приложения
к Плану действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности банка в случае возникновения нестандартных и чрезвычайных ситуаций

Приложение №1 «А»
к Плану ОНиВД

Порядок действий в случае угрозы взрыва (обнаружении подозрительного предмета) и (или) в случае нанесения взрывом ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком

1. Группа безопасности - Начальник Службы безопасности, Начальник дежурной смены.

1.1. При обнаружении угрозы взрыва (подозрительного предмета и т.д.):

1.1.1. Сотрудник дежурной смены:

– сообщить об угрозе взрыва начальнику дежурной смены;

– организовать оцепление вокруг места обнаруженного предмета и обеспечить эвакуацию сотрудников и клиентов Банка на безопасное расстояние.

1.1.2. Начальник дежурной смен»:

– сообщить об угрозе взрыва Начальнику Службы безопасности, дежурному ОВД по телефонам, указанным в Приложении №4.

1.1.3. Начальник Службы безопасности, Начальник дежурной смены:

– обеспечить оцепление подозрительного предмета силами дежурной смены до прибытия сотрудников полиции;

– организовать оповещение руководства Банка;

– организовать встречу спецподразделения полиции;

– встретить прибывшее спецподразделение полиции и обеспечить обследование здания (доступ в помещения Банка, сопровождение);

– при необходимости руководить эвакуацией сотрудников Банка и выносом (вывозом) материальных ценностей из здания совместно с Управляющим делами;

– организовать оповещение сотрудников Банка при помощи громкой связи или иными доступными средствами связи (оповещение организовывает Управляющий делами);

– обеспечить оцепление места обнаружения подозрительного предмета силами дежурной смены до прибытия сотрудников полиции;

– при необходимости руководить эвакуацией сотрудников Банка и выносом (вывозом) материальных ценностей из здания;

– организовать возвращение сотрудников Банка на свои рабочие места в случае соответствующего решения органов МВД и Руководителя ГУЧС.

1.1.4. В случае нанесения взрывом ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– вызвать по телефонам, указанным в Приложении №4, скорую медицинскую помощь и организовать оказание доврачебной медицинской помощи пострадавшим;

– обеспечить эвакуацию и сохранность материальных ценностей;

– действовать по указанию ГУЧС и Начальника Службы безопасности Банка.

1.2. Руководитель ГУЧС:

1.2.1. При объявлении эвакуации:

– покинуть здание путем и в место, указанным Начальником Службы безопасности Банка или прибывшим спецподразделением полиции;

– в случае ликвидации угрозы взрыва и письменного разрешения командира прибывшего спецподразделения полиции принять решение о времени возвращения сотрудников Банка на свои рабочие места и дать соответствующие указания Службе безопасности Банка и Начальнику дежурной смены.

1.2.2. В случае нанесения взрывом ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– созвать Группу управления в чрезвычайных ситуациях (ГУЧС);

– координировать работу ГУЧС;

– координировать обмен информацией с УВД, клиентами Банка, МГТУ Банка России и средствами массовой информации.

1.3. Группа управления в чрезвычайных ситуациях (ГУЧС):

1.3.1. При объявлении эвакуации:

– принять решение о времени возвращения сотрудников Банка на свои рабочие места и дать соответствующие указания Группе безопасности в случае ликвидации угрозы взрыва и письменного разрешения командира прибывшего спецподразделения УВД.

1.3.2. В случае нанесения ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– организовать оказание доврачебной медицинской помощи пострадавшим;

– определить полноту выполнения Плана ОНиВД;

– дать указание Управляющему делами о применении мобильного телефона, приобретенного и хранящегося в ОМТО УД и используемый только для осуществления передачи и получения информации, связанной с угрозой и последствиями взрыва;

– регулярно информировать руководителей структурных подразделений Банка о текущей ситуации;

– принять решение о необходимости возобновления работы Банка в резервном или основном помещении Банка и дать соответствующие указания сотрудникам Службы безопасности, УИТ, Управлению делами и руководителям структурных подразделений Банка;

– временно освободить сотрудников Банка от работы до сообщения информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– в случае необходимости рассмотреть варианты получения сторонней профессиональной помощи от аварийных служб, поставщиков оборудования и ПО;

– в случае необходимости разработать график замещения должностей в зависимости от наличия и работоспособности персонала Банка;

– координировать беседы с кандидатами на прием на работу для скорейшего заполнения всех недостающих вакансий;

– расследовать причины возникновения чрезвычайной ситуации.

1.4. Начальник УИТ, Начальник ОИБ СБ, сотрудники подчиненных структурных подразделений Банка:

1.4.1. При объявлении эвакуации:

– немедленно приостановить работу;

– выключить компьютеры и оргтехнику;

– перенести наиболее важные носители информации, ценности и документы в безопасное место;

– уточнить списки и численность сотрудников Управления, подлежащих эвакуации, и приготовиться к эвакуации из здания Банка;

– эвакуировать сотрудников из занимаемых Банком помещений, маршрутом и в место, указанными ГУЧС или Начальником Службы безопасности Банка;

– пересчитать эвакуированных из занимаемых Банком помещений сотрудников Управления и сообщить об отсутствующих Группе безопасности;

– после сообщения Начальника Службы безопасности Банка о ликвидации угрозы взрыва возобновить деятельность на рабочих местах.

1.4.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– выделить специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями взрыва;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и замены телекоммуникационного оборудования;

– составить график выполнения работ в резервном помещении;

– подготовить и оперативно подключить резервные аппаратные средства и другое оборудование;

– координировать работы, необходимые для восстановления функционирования систем в резервном помещении;

– организовать перевозки запасных частей для замены в резервном помещении;

– организовать перемещение носителей с резервными копиями в резервное помещение;

– организовать (в случае необходимости) работу в резервном помещении с техническим персоналом поставщика;

– определить системную точку для восстановления с резервных копий, восстановить информацию и проверить целостность текущего состояния базы данных;

– восстановить из резервных копий в резервном помещении программное обеспечение, необходимое для возобновления основной деятельности Банка;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– совместно с пользователями подтвердить завершенность операции восстановления базы данных;

– контролировать средства обеспечения безопасности в течение процесса восстановления;

– произвести тестирование прикладных программ;

– начать работу в соответствии с графиком полной загрузки оборудования;

– после завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

1.4.3. В случае принятия решения ГУЧС о возобновлении работы в основном помещении:

– подготовить и оперативно подключить аппаратные средства и другое оборудование, восстановить функции аппаратных средств и другого оборудования АБС или оперативно заменить дефектные узлы резервными в случае отказов;

– координировать работы, необходимые для восстановления функционирования систем в прежнем или резервном помещении;

– организовать перевозки запасных частей для замены в основном помещении;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– начать работу в соответствии с графиком полной загрузки оборудования.

1.4.4. После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

1.5. Управляющий делами, сотрудники Управления делами:

1.5.1. При объявлении эвакуации:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– перенести наиболее важные носители информации, ценности и документы в безопасное место;

– уточнить списки и численность сотрудников Управления, подлежащих эвакуации, и приготовиться к эвакуации из помещений, занимаемых в Банке;

– эвакуировать сотрудников Управления из помещений, занимаемых в Банке маршрутом и в место, указанными ГУЧС и/или Начальником Службы безопасности Банка;

– пересчитать эвакуированных из помещений, занимаемых в Банке сотрудников Управления и сообщить об отсутствующих Группе безопасности;

– после сообщения Начальника группы безопасности о ликвидации угрозы взрыва возобновить деятельность на рабочих местах.

1.5.2. Отдел связей с общественностью и рекламы Управления делами, Административный отдел Управления делами:

– осуществить оповещение сотрудников и заинтересованных лиц Банка доступными средствами связи;

– по решению ГУЧС разместить необходимую информацию на сайте Банка.

1.5.3. Отдел по работе с персоналом:

– перенести наиболее важные носители информации, ценности и документы, трудовые книжки сотрудников Банка, в безопасное место;

– уточнить списки и численность сотрудников структурного подразделения Банка, подлежащих эвакуации, и приготовиться к эвакуации из помещений, занимаемых в Банке.

1.5.4. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

1.5.4.1. Отдел материально-технического обеспечения:

– совместно с УИТ выделить специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями взрыва;

– оценить ущерб, причиненный помещениям и имуществу Банка, составить и проанализировать список потребностей;

– уведомить поставщиков о чрезвычайной ситуации и информировать их об адресе резервного помещения;

– координировать работы по ремонту или подготовке нового постоянного помещения в первоначальном или новом месте;

– обеспечить транспортом и материально-техническими средствами и организовать совместно со Службой Безопасности Банка перевозку персонала и ценностей в резервное помещение;

– организовать размещение персонала, материалов и оборудования в резервных помещениях;

– обеспечить энергоснабжение, подводку необходимого электрического питания, кабелей и соединителей;

– совместно с УИТ обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и замены телекоммуникационного оборудования;

– обеспечить дополнительные офисные помещения мебелью и другим офисным оборудованием.

1.6. Финансовый директор, сотрудники ФАУ:

1.6.1. При объявлении эвакуации:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– перенести используемые носители информации, ценности в безопасное место;

– уточнить списки и численность сотрудников Управления, подлежащих эвакуации, и приготовиться к эвакуации из помещений, занимаемых в Банке;

– эвакуировать сотрудников Управления из помещений, занимаемых в Банке маршрутом и в место, указанными ГУЧС и/или Начальником Службы безопасности Банка;

– пересчитать эвакуированных из помещений, занимаемых в Банке сотрудников Управления и сообщить об отсутствующих Группе безопасности;

– после сообщения ГУЧС о ликвидации угрозы взрыва возобновить деятельность на рабочих местах.

1.6.2. В случае нанесения взрывом ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– проанализировать возникший в результате взрыва ущерб и направить в страховую компанию запрос на проведение его оценки;

– обработать все поступившие заявления об ущербе;

– предоставить Руководителю ГУЧС подробный отчет об ущербе;

– подготовить совместно с Начальником УПО требования к виновным лицам, а также к страховой компании о возмещении ущерба;

1.7. Управление правового обеспечения (УПО):

1.7.1. При объявлении эвакуации:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

1.7.2. В случае нанесения взрывом ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– обеспечить сохранность правоустанавливающих, учредительных и регистрационных документов Банка, документов по эмиссиям Банка, протоколов заседания Наблюдательного совета и Общего собрания акционеров Банка, а также Комитета по проблемным активам;

– подготовить совместно с Финансовым директором, Службой безопасности требования к виновному лицу, страховой компании о возмещении ущерба;

– обеспечить сохранность (перенести в безопасное место, убрать в сейф и т.д.) правоустанавливающих, учредительных и регистрационных документов Банка, Уставные документы, лицензии, документы по эмиссиям Банка;

– запереть металлические шкафы с юридическими делами клиентов;

– запереть в металлические шкафы и сейфы документы, используемые в работе, в том числе доверенности на сотрудников УПО и штампы;

– убрать в сейф печати и штампы, используемые для заверения документов;

– обеспечить представление интересов Банка в суде и взаимодействие со Службой судебных приставов;

– уведомить налоговые органы о возникновении чрезвычайной ситуации в случае невозможности своевременной отправки информации, предусмотренной налоговым кодексом.

1.8. Управление по работе с корпоративными клиентами, Управление развития банковских услуг, Центр электронных услуг и обслуживания физических лиц:

– немедленно приостановить работу;

– обеспечить сохранность (перенести в безопасное место, убрать в сейф и т. д.) документов, содержащих конфиденциальную информацию;

– запереть в металлические шкафы и сейфы документы и используемые в работе печати и штампы;

– убрать в сейф печати и штампы, используемые для заверения документов;

– согласовать порядок отправки платежей с Казначейством ,Отделом расчетных систем и банковских телекоммуникаций, Операционным отделом Управления «Расчетный центр», УИТ и Центром электронных услуг и обслуживания физических лиц.

– при невозможности продолжать деятельность в штатном режиме, информировать клиентов Банка о сложившихся непредвиденных обстоятельствах (чрезвычайной ситуации) возможными способами: по мобильному телефону, SMS, объявление и др.

1.9. Управление «Расчетный центр»:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– обеспечить сохранность (перенести в безопасное место, убрать в сейф и т. д.) документов, содержащих конфиденциальную информацию, и используемые в работе печати и штампы;

– обеспечить согласование порядка отправки платежей с Казначейством, Операционным отделом, Отделом расчетных систем и банковских телекоммуникаций, УИТ и Центром электронных услуг и обслуживания физических лиц.

– обеспечить совместно с Управлением по работе с корпоративными клиентами, Управлением развития банковских услуг (Отдел по работе с VIP-клиентами) согласование порядка уведомления клиентов, контрагентов и налоговые органы о возникновении чрезвычайной ситуации;

– организовать осуществление (проведение) платежей и кассовой работы.

1.10. Отдел открытия счетов Управления «Расчетный центр»:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– запереть металлические шкафы с юридическими делами клиентов;

– запереть в металлические шкафы и сейфы документы и используемые в работе печати и штампы.

1.11. Операционный отдел Управления «Расчетный центр»:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– согласовать порядок отправки платежей с Казначейством, Отделом расчетных систем и банковских телекоммуникаций, УИТ и Центром электронных услуг и обслуживания физических лиц;

– совместно с Управлением по работе с корпоративными клиентами оперативно информировать клиентов о возникшей ситуации и об изменениях в порядке работы путем оповещения по телефону, системе «Банк-Клиент», объявлениями в операционном зале Банка.

– обеспечить сохранность (перенести в безопасное место, убрать в сейф и т. д.) документы и используемые в работе печати и штампы.

1.12. Центральная операционная касса:

– Заведующему кассой принять у кассиров все остатки денежных средств, поместить их в хранилище, хранилище закрыть и сдать под охрану;

– в случае принятия решения ГУЧС о возобновлении работы в резервном помещении совместно со Службой Безопасности Банка и службой инкассации НКО «ИНКАХРАН» (АО) обеспечить перевозку ценностей из хранилища.

2. Все сотрудники Банка.

2.1. При объявлении эвакуации:

– немедленно приостановить работу;

– выключить из электросети компьютеры и оргтехнику;

– перенести наиболее важные носители информации, ценности и документы в безопасное место;

– покинуть, занимаемые в Банке помещения, эвакуировать посетителей, находящихся в структурных подразделениях, из помещений, занимаемых в Банке маршрутом и в место, указанными Службой безопасности Банка;

– покидая помещение, спускаться по лестнице;

– пресекать панику, давку в дверях при эвакуации;

– оказавшись на улице, не стоять вблизи зданий, перейти на открытое пространство;

– пересчитать эвакуированных из помещений, занимаемых Банком сотрудников структурного подразделения Банка и сообщить об отсутствующих Службе безопасности;

– после сообщения Начальника Службы безопасности Банка о ликвидации угрозы взрыва возобновить деятельность на рабочих местах;

– в случае принятия решения ГУЧС о возобновлении работы в резервном помещении ждать информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

2.2. В случае невозможности выйти из помещений, занимаемых Банком я и угрозы его обрушения:

– открыть дверь из помещения, чтобы обеспечить себе выход в случае необходимости;

– занять самое безопасное место: проемы капитальных внутренних стен, углы, образованные капитальными внутренними стенами, под балками каркаса;

– при возможности, спрятаться под стол – он защитит от падающих предметов и обломков;

– держаться подальше от окон, электроприборов;

– не поддаваться панике и сохранять спокойствие, ободрять присутствующих.

2.3. В случае обрушения помещения, занимаемого Банком и попадания под завал:

– глубоко дышать, не поддаваться панике и не падать духом, сосредоточиться на самом важном, пытаться выжить любой ценой;

– по возможности оказать себе первую медицинскую помощь;

– постараться определить, где Вы находитесь, нет ли рядом других людей: прислушаться, подать голос;

– поискать в карманах или поблизости предметы, которые могли бы помочь подать световые или звуковые сигналы (например, фонарик, зеркальце, а также металлические предметы, которыми можно постучать по трубе или стене и тем самым привлечь внимание);

– если единственным путем выхода является узкий лаз – протиснуться через него. Для этого необходимо расслабить мышцы и двигаться, прижав локти к телу.

2.4. Признаки, которые могут указывать на наличие взрывного устройства:

– наличие на обнаруженном предмете проводов, веревок, изоленты;

– подозрительные звуки, щелчки, тиканье часов, издаваемые предметом;

– от предмета исходит характерный запах миндаля или другой необычный запах.

Причины, служащие поводом для опасения:

– нахождение подозрительных лиц до обнаружения этого предмета;

– угрозы лично, по телефону или в почтовых отправлениях.

Приложение №1 «Б»
к Плану ОНиВД

Порядок действий в случае нападения на персонал и собственность Банка

1. Группа безопасности - Начальник Службы безопасности Банка, Начальник дежурной смены.

1.1. Начальник дежурной смены:

– организовать отражение нападения силами дежурной смены;

– вызвать наряд полиции при помощи кнопки тревожной сигнализации;

– блокировать главный и служебный входы при помощи магнитных замков;

– сообщить о факте нападения по телефонам, указанным в Приложении №4, в дежурную часть ГУВД г. Москвы, Начальнику Службы безопасности Банка, через Управление делами руководству Банка;

– по команде Начальника Службы безопасности Банка, с использованием громкой связи, оповестить сотрудников Банка.

1.2. Начальник Службы безопасности Банка, Начальник дежурной смены:

– организовать оповещение сотрудников Банка при помощи громкой связи, Управляющий делами организует оповещение сотрудников Банка иными доступными средствами связи;

– в случае необходимости произвести эвакуацию сотрудников Банка из помещений, занимаемых Банком;

– обеспечить сохранность и неизменность возможных улик;

– в случае необходимости вызвать по телефонам, указанным в Приложении №4, скорую медицинскую помощь и организовать оказание доврачебной медицинской помощи пострадавшим;

– не выпускать лиц, присутствовавших при чрезвычайном происшествии, из помещений, занимаемых Банком, за исключением нуждающихся в срочной медицинской помощи;

– не впускать в помещения Банка, никого из посторонних лиц, за исключением сотрудников правоохранительных органов;

– не делать никаких заявлений для прессы и других средств массовой информации без консультаций с юристами до тех пор, пока правоохранительные органы не выполнят все предусмотренные законом следственные действия;

– подготовить для ГУЧС и органов полиции информацию, которая содержит следующие параметры:

– количество лиц, вовлеченных в происшествие, с указанием их фамилий и адресов (сотрудники Банка, потерпевшие клиенты, свидетели происшествия, случайные прохожие и т. п.);

– сведения о террористах и грабителях, их приметы, направление их побега, использованные для этого средства транспорта;

– сведения о сотрудниках охранного предприятия, обеспечивающего охрану Банка;

– информацию о потерпевших лицах, состоянии их здоровья, принятых мерах по оказанию им первой медицинской помощи с указанием адресов больниц и клиник в случаях их госпитализации и стационарного лечения;

– в дальнейшем действовать по указанию ГУЧС и начальника Службы безопасности Банка.

1.3. Руководитель ГУЧС:

– созвать Группу управления в чрезвычайных ситуациях (ГУЧС);

– координировать обмен информацией с УВД, клиентами Банка, МГТУ Банка России и средствами массовой информации.

1.4. Группа управления в чрезвычайных ситуациях (ГУЧС):

– корректировать график замещения должностей в зависимости от наличия и работоспособности персонала Банка;

– координировать прием на работу, для скорейшего заполнения всех недостающих вакансий;

– координировать общение с клиентами, ЦБ РФ и средствами массовой информации;

– определить полноту выполнения Плана ОНиВД в случае возникновения непредвиденных обстоятельств (чрезвычайных ситуации);

– расследовать причины возникновения чрезвычайной ситуации;

– составить Отчет, содержащий предложения по совершенствованию Плана действий в случае возникновения нестандартных и чрезвычайных ситуаций.

1.5. Начальник УИТ, Начальник ОИБ СБ, Начальник ОМТО УД, сотрудники подчиненных структурных подразделений Банка после разрешения деятельности начальником Службы безопасности Банка:

– в случае повреждений подготовить и оперативно подключить аппаратные средства и другое оборудование, восстановить функции аппаратных средств и другого оборудования АБС или оперативно заменить дефектные узлы резервными в случае отказов;

– организовать перевозки запасных частей;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– начать работу в соответствии с графиком полной загрузки оборудования;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования;

– о результатах восстановления информировать ГУЧС.

1.6. Управления делами:

– после разрешения деятельности Начальником Службы безопасности Банка:

– оценить ущерб, причиненный помещениям и имуществу Банка, составить и проанализировать список потребностей;

– обеспечить работы по ремонту помещения;

– организовать перевозки и размещение персонала, материалов и оборудования;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования;

– в случае необходимости обеспечить помещения мебелью и другим офисным оборудованием.

1.7. УПО:

– совместно с ФАУ и Службой безопасности проанализировать причины возникшего в результате нападения ущерба, по возможности осуществлять взаимодействие с правоохранительными органами по вопросам установления виновных лиц, направить соответствующие претензии, в том числе в страховую компанию запрос на проведение оценки ущерба;

– обработать все поступившие заявления об ущербе;

– предоставить Руководителю ГУЧС подробный отчет об ущербе;

– обеспечить представление интересов Банка в суде и иных государственных органах.

2. Сотрудники Банка.

2.1. В случае нападения с целью ограбления:

– по возможности нажать на тревожную кнопку;

– по возможности дать другим сотрудникам Банка сигнал о том, что совершается нападение, но помнить, что делать это нужно с величайшей осторожностью. Не делать ничего, что может спровоцировать агрессивные действия преступников;

– подчиняться всем требованиям нападающих;

– не пытаться спорить с нападающими, чтобы не спровоцировать их на агрессию;

– отдавать нападающим только то, что он сам требует;

– постараться запомнить любую информацию о нападающих (количество, вооружение, внешний вид, особенности внешности, телосложения, акцента, клички, шрамы, татуировки, тематика разговора, темперамент, манера поведения);

– следить за тем, к чему прикасаются преступники. Это поможет быстрее получить отпечатки их пальцев;

– сообщать нападающим заранее обо всех своих действиях, которые собираетесь совершить. Если, например, вам необходимо сделать шаг или протянуть руку, сообщить грабителю об этом заранее, иначе он может неправильно понять Ваши движения.

2.2. В случае захвата заложников:

– постараться запомнить любую информацию о нападающих (количество, вооружение, внешний вид, особенности внешности, телосложения, акцента, клички, шрамы, татуировки, тематика разговора, темперамент, манера поведения);

– не допускать действий, которые могут спровоцировать нападающих к применению оружия и привести к человеческим жертвам;

– переносить лишения, оскорбления и унижения. Не смотреть в глаза преступникам, не вести себя вызывающе;

– при необходимости выполнять требования преступников, не противоречить им, не рисковать жизнью окружающих и своей собственной;

– стараться не допускать истерик и паники;

– на совершение любых действий (сесть, встать, попить, сходить в туалет) спрашивать разрешение;

– в случае ранения постараться не двигаться, чтобы сократить потерю крови.

2.3. Во время проведения спецслужбами операции по освобождению заложников неукоснительно соблюдать следующие требования:

– лежать на полу лицом вниз, закрыть голову руками и не двигаться;

– ни в коем случае не бежать навстречу сотрудникам спецслужб или от них, так как они могут принять Вас за преступника;

– если есть возможность, держаться подальше от проемов дверей и окон.

Приложение №1 «В»
к Плану ОНиВД

Порядок действий в случае пожарной тревоги

Основными факторами, влияющими на непрерывность деятельности Банка, при пожаре являются:

– невозможность доступа в помещения, занимаемые Банком (структурные подразделения Банка) и проведения всех операций;

– возможные повреждения оборудования, документов;

– возможные травмы сотрудников Банка;

– возможность обрушения здания.

Основными опасными факторами пожара являются:

– тепловое излучение;

– высокая температура;

– отравляющее действие дыма (продуктов сгорания: окиси углерода и др.);

– снижение видимости при задымлении.

На случай пожара в помещениях, занимаемых Банком предусмотрена пожарная сигнализация, которая при первых признаках возгорания и (или) задымления подает звуковой сигнал, начинает тушение путем разбрызгивания воды.

На случай возможной порчи, в Банке принято копирование основных, наиболее важных документов и хранение их в специальных несгораемых сейфах либо в отдельных помещениях.

1. Группа безопасности - Начальник Службы безопасности Банка, Начальник дежурной смены.

1.1. Начальник дежурной смены:

– сообщить о возникновении пожара по телефонам, указанным в Приложении №4;

– силами дежурной смены организовать тушение очага возгорания, используя средства пожаротушения на этажах здания;

– сообщить начальнику Службы безопасности Банка и через Управление делами руководству Банка о возникновении пожара, а также руководителю арендодателя.

1.2. Начальник Службы безопасности Банка, Начальник дежурной смены:

– организовать оповещение сотрудников Банка при помощи громкой связи о месте очага возгорания и путях эвакуации из помещений, занимаемых Банком, Управляющий делами организует оповещение сотрудников Банка иными доступными средствами связи;

– в случае угрозы жизни людей немедленно организовать их спасание, используя для этого имеющиеся силы и средства;

– при необходимости вызвать по телефонам, указанным в Приложении №4, скорую медицинскую помощь и организовать оказание доврачебной медицинской помощи пострадавшим;

– удалить за пределы опасной зоны всех сотрудников Банка, не участвующих в тушении пожара;

– совместно с руководителями служб и управлений Банка организовать спасение и охрану материальных ценностей Банка;

– до прибытия пожарных расчетов в чрезвычайном режиме обеспечить эвакуацию припаркованного автотранспорта вокруг здания, занимаемого Банком, с целью беспрепятственного подъезда к зданию пожарных автомашин;

– встретить подразделения пожарной охраны и оказать помощь в выборе кратчайшего пути для подъезда к очагу пожара;

– информировать руководителя подразделения пожарной охраны о конструктивных и технологических особенностях здания, прилегающих строений и сооружений, количестве и пожароопасных свойствах хранимых и применяемых веществ, материалов, изделий и других сведениях, необходимых для успешной ликвидации пожара;

– в дальнейшем действовать по указанию ГУЧС и начальника Службы безопасности Банка.

1.3. Руководитель ГУЧС:

– созвать Группу управления в чрезвычайных ситуациях (ГУЧС);

– координировать обмен информацией с клиентами Банка, МГТУ Банка России и средствами массовой информации.

1.3.1. Группа управления в чрезвычайных ситуациях (ГУЧС).

1.3.1.1. При объявлении эвакуации:

– принять решение о времени возвращения сотрудников Банка на свои рабочие места.

1.3.1.2. В случае нанесения пожаром ущерба здоровью сотрудников, оборудованию и помещениям, занимаемым Банком:

– определить полноту выполнения Плана ОНиВД;

– дать указания Управлению делами и УИТ выделить специальный канал связи (отдельный телефонный номер (номера)), используемого только для осуществления передачи и получения информации, связанной с последствиями пожара;

– регулярно информировать руководителей структурных подразделений Банка о текущей ситуации;

– принять решение о необходимости возобновления работы Банка в резервном или основном помещении Банка и дать соответствующие указания руководителям структурных подразделений Банка.

– временно освободить сотрудников Банка от работы до сообщения информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– в случае необходимости рассмотреть варианты получения сторонней профессиональной помощи от аварийных служб, поставщиков оборудования и программного обеспечения;

– корректировать график замещения должностей в зависимости от наличия и работоспособности персонала Банка;

– координировать беседы с кандидатами на прием на работу, для скорейшего заполнения всех недостающих вакансий;

– расследовать причины возникновения чрезвычайной ситуации.

1.4. УИТ.

1.4.1. При обнаружении пожара или дыма в помещениях Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– попытаться погасить пожар ручным огнетушителем (расположение огнетушителей указано на Плане эвакуации);

– выключить компьютеры, работа которых некритична для работы Банка;

Если не удается погасить пожар:

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– приготовиться к экстренной эвакуации.

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– закрыть все оборудование большими пластиковыми пленками или листами.

– эвакуировать сотрудников Управления из помещения, занимаемого в Банке маршрутом и в место, указанными Группой безопасности;

– пересчитать эвакуированных из помещения, занимаемого в Банке сотрудников Управления и сообщить об отсутствующих Группе безопасности;

– после сообщения Начальника группы безопасности о ликвидации пожара возобновить деятельность на рабочих местах;

– в случае принятия решения ГУЧС о возобновлении работы в резервном помещении, ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

1.4.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– составить график выполнения работ в резервном помещении;

– выделить совместно с Управляющим делами специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями пожара;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования

– подготовить и оперативно подключить резервные аппаратные средства и другое оборудование;

– координировать работы, необходимые для восстановления функционирования систем в резервном помещении;

– организовать перевозки запасных частей для замены в резервном помещении;

– организовать перемещение носителей с резервными копиями в резервное помещение;

– организовать работу в резервном помещении с техническим персоналом поставщика (по мере необходимости);

– определить системную точку для восстановления с резервных копий, восстановить информацию и проверить целостность текущего состояния базы данных;

– инсталлировать в резервном помещении программное обеспечение, необходимое для возобновления основной деятельности Банка;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– совместно с пользователями подтвердить завершенность операции восстановления базы данных;

– контролировать средства обеспечения безопасности в течение процесса восстановления;

– произвести тестирование прикладных программ;

– начать работу в соответствии с графиком полной загрузки оборудования.

После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

1.4.3. В случае принятия решения ГУЧС о возобновлении работы в основном помещении:

– подготовить и оперативно подключить аппаратные средства и другое оборудование, восстановить функции аппаратных средств и другого оборудования АБС или оперативно заменить дефектные узлы резервными в случае отказов;

– координировать работы, необходимые для восстановления функционирования систем в прежнем или резервном помещении;

– организовать перевозки запасных частей для замены в основном помещении;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– начать работу в соответствии с графиком полной загрузки оборудования.

1.4.4. После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

1.5. Управление делами.

1.5.1. При обнаружении пожара или дыма в помещениях Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– попытаться погасить пожар ручным огнетушителем;

– сообщить в Службу безопасности Банка;

– выключить компьютеры и оргтехнику;

Если не удается погасить пожар:

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– приготовиться к экстренной эвакуации.

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– покрыть все оборудование большими пластиковыми пленками или листами.

– эвакуировать сотрудников Управления из помещений, занимаемых в Банке маршрутом и в место, указанными Службой безопасности Банка;

– пересчитать эвакуированных из помещений, занимаемых в Банке сотрудников Управления и сообщить об отсутствующих Службе безопасности Банка;

– после сообщения Начальника группы безопасности о ликвидации пожара возобновить деятельность на рабочих местах;

– в случае принятия решения ГУЧС о возобновлении работы в резервном помещении ждать информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

1.5.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– выделить совместно с УИТ специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями пожара;

– совместно с ФАУ оценить ущерб, причиненный помещениям и имуществу Банка, составить и проанализировать список потребностей;

– уведомить поставщиков о чрезвычайной ситуации и информировать их об адресе резервного помещения;

– координировать работы по ремонту или подготовке нового постоянного помещения в первоначальном или новом месте;

– организовать перевозки и размещение людей, материалов и оборудования в резервных помещениях;

– обеспечить энергоснабжение, подводку необходимого электрического питания, кабелей и соединителей;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования;

– обеспечить дополнительные офисные помещения мебелью и другим офисным оборудованием.

1.6. УПО.

1.6.1. При обнаружении пожара или дыма в помещениях Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– попытаться погасить пожар ручным огнетушителем;

– сообщить в Службу безопасности Банка;

– выключить компьютеры и оргтехнику;

Если не удается погасить пожар:

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– приготовиться к экстренной эвакуации.

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– обеспечить сохранность правоустанавливающих, учредительных и регистрационных документов Банка, документов по эмиссиям Банка, протоколов заседания Наблюдательного совета, Общего собрания акционеров Банка, Комитета по проблемным активам;

– закрыть все оборудование большими пластиковыми пленками или листами, при их наличии;

– эвакуировать сотрудников Управления и посетителей, находящихся в подразделении и переговорных комнатах, из помещений, занимаемых в Банке маршрутом и в место, указанными Службой безопасности Банка;

– пересчитать эвакуированных из помещений, занимаемых в Банке сотрудников Управления и сообщить об отсутствующих Службе безопасности Банка;

– после сообщения Начальника Службы безопасности Банка о ликвидации пожара возобновить деятельность на рабочих местах;

1.6.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– совместно с ФАУ проанализировать возникший в результате пожара ущерб и направить в страховую компанию запрос на проведение его оценки;

– обработать все поступившие заявления об ущербе;

– предоставить Руководителю ГУЧС подробный отчет об ущербе;

– подготовить требования к страховой компании о возмещении ущерба;

– обеспечить представление интересов Банка в суде и взаимодействие со Службой судебных приставов.

1.7. Все сотрудники Банка.

1.7.1. При обнаружении пожара или дыма в помещениях Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– попытаться погасить пожар ручным огнетушителем;

– сообщить в Службу безопасности Банка;

– выключить из электросети компьютеры и оргтехнику;

Если не удается погасить пожар:

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– приготовиться к экстренной эвакуации.

Если время позволяет:

– перенести используемые носители информации, денежные средства и ценности, наиболее важные документы и ценное имущество в безопасное место;

– закрыть все оборудование большими пластиковыми пленками или листами при их наличии;

– запереть металлические шкафы документы;

– убрать в сейф печати и штампы, используемые для заверения документов.

– оказать содействие в эвакуации сотрудников подразделений Банка и посетителей, находящихся в подразделениях и переговорных комнатах, из помещений, занимаемых Банком маршрутом и в место, указанными Службой безопасности Банка;

– после сообщения Начальника Службы безопасности Банка о ликвидации пожара возобновить деятельность на рабочих местах.

1.7.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

2. УИТ, ОИБ СБ, Управляющий делами, сотрудники Управления делами, Управление по работе с корпоративными клиентами, Управление развития банковских услуг, Центр электронных услуг и обслуживания физических лиц, Управление «Расчетный центр»:

– осуществить мероприятия с учетом особенности выполняемых конкретным подразделением функций (согласно пунктам 1.4.2, 1.5.4, 1.8, 1.9, 1.13 Приложения №1 «А»)

3. Особенности осуществления Плана ОНиВД в случае пожара в Головном офисе Банка на арендуемых площадях по адресу: _____ и взаимодействия с сотрудниками арендодателя по отключению подачи электроэнергии в структурном подразделении Банка, в котором обнаружен пожар, оповестить руководителю арендодателя.

№	Действия	Комментарий	Исполнитель	Сроки исполнения
1	Подать голосом сигнал **«пожар»**	В случае, если рядом находятся сотрудники Банка, их необходимо оповестить о пожаре. Оповестить начальника Службы безопасности Банка	Сотрудник Банка, обнаруживший пожар	Немедленно
2	Оповещение пожарной части, ответственного сотрудника арендодателя и руководителя ГУЧС Банка	Необходимо точно указать адрес Банка (подразделения Банка), указать, где конкретно произошло возгорание, назвать себя (фамилия, должность)	Начальник Службы безопасности Банка	Немедленно
3	Организовать локализацию и тушение пожара имеющимися силами и средствами во взаимодействии с ответственным сотрудником арендодателя	В арендуемых помещениях Банк установлены следующие системы пожарной безопасности: - система пожарной сигнализации (при возникновении задымления включается звуковой сигнал в службу охраны с указанием места задымления); - система оповещения о пожаре – через громкоговорители, установленные в каждом кабинете и коридорах, звучит сообщение: **«Внимание пожарная тревога. Всем немедленно покинуть здание»** (включается при срабатывании системы сигнализации); - арендуемые помещения укомплектованы огнетушителями, которые находятся в специальных местах на каждом этаже. В случае пожара сотрудники Банка могут	Ответственный сотрудник арендодателя, отвечающий за пожарную безопасность и сотрудники Банка в помещении, где произошло возгорание	Немедленно

		воспользоваться огнетушителями.		
4	Отключить подачу электроэнергии в структурное подразделение Банка	Руководитель ГУЧС отдает распоряжение на отключение подачи электроэнергии.	Сотрудник арендодателя, обслуживающий арендуемые помещения	Немедленно
5	Объявление срочной эвакуации	Объявлять следует спокойно, стараясь не вызывать паники среди сотрудников и посетителей Банка; объявлять во всех помещениях.	Начальник Службы безопасности Банка	Немедленно
6	Эвакуировать людей из прилегающих к месту пожара помещений	При срабатывании системы пожарной сигнализации и системы оповещения о пожаре пассажирский лифт опускается на первый этаж, открывает двери и отключается (эвакуация сотрудников в данном случае при помощи лифта запрещена). Эвакуация сотрудников Банка осуществляется по пожарной (запасной) лестнице.	Начальник и сотрудники Службы безопасности Банка, сотрудники арендодателя, обслуживающие арендуемые помещения	Немедленно
7	Организовать тщательную проверку всех задымленных и горящих помещений с целью выявления пострадавших или потерявших сознание, оказать пострадавшим первую медицинскую помощь		Начальник и сотрудники Службы безопасности Банка и ОМТО, сотрудники арендодателя, обслуживающие арендуемые помещения	Немедленно
8	Эвакуация наиболее значимого оборудования из серверной	Список и последовательность (по значимости) эвакуации оборудования приведен в приложении.	Сотрудники Управления информационных технологий	Немедленно
9	Эвакуация документации и имущества из прилегающих к месту пожара помещений	Выносятся наиболее значимые документы.	Сотрудники соответствующих подразделений, сотрудники Службы безопасности Банка и ОМТО помогают в эвакуации документов	Немедленно
10	Сверка списочного количества с фактическим наличием эвакуированных людей из помещений, занимаемых Банком	Все эвакуированные из здания люди пересчитываются, и наличие их сверяется с имеющимися поименными списками.	Начальник Службы безопасности Банка, Начальник отдела по работе с персоналом, руководители структурных подразделений Банка	Немедленно после окончания эвакуации
11	Организовать охрану вынесенного имущества и документации		ОМТО УД	
12	Встреча пожарных подразделений	Место встречи - основная дорога к Банку. Встречающий сотрудник обязан сообщить старшему команды сведения об очаге пожара, принятых мерах и особенностях помещений Банка (структурного подразделения Банка), которые могут повлиять на развитие и ликвидацию пожара.	Служба безопасности Банка	С начала выноса
13	Оповещение заинтересованных лиц	Необходимо оповестить: - территориальное отделение Банка России (тел. в Приложении №4); - акционеров, участников; - клиентов Банка (размещение	В соответствии с Приложением №3	Немедленно

		объявления) с указанием предполагаемых сроков восстановления работы Банка.		
14	Оценка возможности начала осуществления критических операций в течение операционного дня	По результатам оценки принимается решение о возобновлении критических операций в сокращенном либо полном режиме в помещении Банка или проведении их в резервном помещении на резервном оборудовании в сокращенном режиме.	ГУЧС	Немедленно
15	Проведение критических операций в чрезвычайном режиме	Критические операции производятся строго в соответствии с действующим законодательством без изменения технологии в порядке и на основе ресурсов, определенных решением ГУЧС в соответствии со сложившимися обстоятельствами.	Сотрудники соответствующих подразделений Банка	По принятии решения ГУЧСГ

4. План выхода из кризисной ситуации при пожаре:

4.1. Участники ГУЧС оценивают возможность продолжения проведения основных операций в основном помещении в полном (сокращенном) объеме.

4.2. В случае, если помещение пострадало несущественно и продолжение всех операций возможно в основном помещении, руководитель ГУЧС принимает решение о прекращении работы в чрезвычайном режиме и переходе в обычный режим работы. Решение оформляется приказом руководителя ГУЧС.

4.3. В случае, если имеется возможность проводить основные операции в сокращенном режиме, то руководитель ГУЧС принимает решение о проведении операций в сокращенном режиме (указывается, в чем именно заключается сокращенный режим) и восстановлении помещений Банка. По завершении восстановления помещений руководитель ГУЧС принимает решение прекращении работы в чрезвычайном режиме и переходе в обычный режим работы. Решение оформляется приказом.

4.4. В случае, если основное помещение Банка пострадало существенно и продолжение работы в нем невозможно, руководитель ГУЧС принимает решение о немедленном переносе проведения критических операций в резервном помещении и восстановлении основных помещений. По мере проведения восстановительных работ проведение критических операций переносится в основные помещения Банка. При полном восстановлении всех процессов ГУЧС принимает решение о завершении работы в кризисном режиме приказом руководителя ГУЧС.

4.5. Во втором и третьем случае заинтересованные стороны оповещаются о принятом решении в порядке, изложенном выше.

Приложение №1 «Г»
к Плану ОНиВД

Порядок действий в случае эпидемий

1. Группа безопасности - Начальник Службы безопасности Банка, Начальник дежурной смены:

– ограничить передвижение людей в (из) зараженную зону;

– при угрозе жизни и здоровью, эвакуировать персонал и клиентов Банка в безопасную зону;

– в случае принятия решения Группой управления в чрезвычайных ситуациях (ГУЧС) (Правление Банка) об обращении к кадровым агентствам, оказать содействие кадровому аппарату в проверке кандидатов на работу.

2. Руководитель ГУЧС принимает решение об эвакуации персонала или объявлении карантина.

3. Группа управления в чрезвычайных ситуациях (ГУЧС) (Правление Банка):

– составить график замещения должностей;

– при необходимости принять решение об обращении к кадровым агентствам для подбора персонала на временную работу.

4. УИТ и ОИБ СБ:

– наделить вновь принятых сотрудников Банка правами доступа в соответствии с графиком замещения должностей.

5. Управление делами:

– произвести инструктаж в соответствии с Планом ОНиВД принятых на работу сотрудников Банка;

– обеспечить принятых на работу сотрудников Банка рабочими принадлежностями.

6. Все сотрудники Банка:

– применить меры индивидуальной защиты;

– известить курирующего Вице-президента и Управление делами;

– обеспечить сохранность используемых носителей информации;

– выключить компьютеры;

– отключить электроприборы, кондиционеры;

– запереть в металлические шкафы и сейфы документы и используемые в работе печати и штампы;

– после сообщения о ликвидации угрозы эпидемии возвратиться на свои места и возобновить деятельность.

Приложение №1 «Д»
к Плану ОНиВД

Порядок действий в случае затопления

1. Группа безопасности - Начальник Службы безопасности Банка, Начальник дежурной смены:

– начальнику дежурной смены охраны сообщить начальнику Службы безопасности Банка и через Управление делами руководству Банка, а также руководителю арендодателя;

– при необходимости, совместно с Управлением делами, обеспечить эвакуацию сотрудников, клиентов банка и материальных ценностей из затапливаемых помещений;

– организовать охрану эвакуированных материальных ценностей;

– в дальнейшем действовать по указанию начальника Службы безопасности Банка.

2. Руководитель ГУЧС

– принять решение об эвакуации персонала.

3. Группа управления в чрезвычайных ситуациях (ГУЧС).

3.1. При объявлении эвакуации:

– принять решение о времени возвращения сотрудников Банка на свои рабочие места.

3.2. В случае нанесения затоплением повреждений оборудованию и помещениям, занимаемым Банком:

– определить полноту выполнения Плана ОНиВД;

– дать указание Управляющему делами о применении мобильного телефона, приобретенного и хранящегося в ОМТО УД и используемый только для осуществления передачи и получения информации, связанной с угрозой и последствиями затопления;

– регулярно информировать руководителей структурных подразделений Банка о текущей ситуации;

– принять решение о необходимости возобновления работы Банка в резервном или основном помещении Банка и дать соответствующие указания руководителям структурных подразделений Банка.

– при затоплении здания временно освободить сотрудников Банка от работы до сообщения информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– в случае необходимости рассмотреть варианты получения сторонней профессиональной помощи от аварийных служб, поставщиков оборудования и программного обеспечения;

– расследовать причины возникновения чрезвычайной ситуации.

4. УИТ.

4.1. При обнаружении поступления воды в помещения Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– сообщить в Управление делами;

– выключить компьютеры, работа которых некритична для работы Банка;

– выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– закрыть все оборудование большими пластиковыми пленками или листами;

– при угрозе жизни и здоровью сотрудникам Управления эвакуироваться из помещений, занимаемых Банком маршрутом в место определенное Службой безопасности Банка;

– после сообщения о ликвидации угрозы или последствий затопления возобновить деятельность на рабочих местах;

– в случае затопления коммуникационных колодцев или точек подключения систем связи вызвать сервисных инженеров, обслуживающих подвергшиеся затоплению технические средства,

осмотреть оборудование для определения ущерба от поступления воды прежде, чем оно будет включено снова;

– при невозможности продолжать работу в обычном режиме ждать от ГУЧС информации о местонахождении нового рабочего места и возобновить деятельность в указанном резервном помещении.

4.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– составить график выполнения работ в резервном помещении;

– подготовить и оперативно подключить резервные аппаратные средства и другое оборудование;

– координировать работы, необходимые для восстановления функционирования систем в резервном помещении;

– организовать перевозки запасных частей для замены в резервном помещении;

– организовать перемещение носителей с резервными копиями в резервное помещение;

– организовать работу в резервном помещении с техническим персоналом поставщика (по мере необходимости);

– определить системную точку для восстановления с резервных копий, восстановить информацию и проверить целостность текущего состояния базы данных;

– инсталлировать в резервном помещении программное обеспечение, необходимое для возобновления основной деятельности Банка;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– совместно с пользователями подтвердить завершенность операции восстановления базы данных;

– контролировать средства обеспечения безопасности в течение процесса восстановления;

– произвести тестирование прикладных программ;

– начать работу в соответствии с графиком полной загрузки оборудования.

После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

4.3. В случае принятия решения ГУЧС о возобновлении работы в основном помещении:

– подготовить и оперативно подключить аппаратные средства и другое оборудование, восстановить функции аппаратных средств и другого оборудования АБС или оперативно заменить дефектные узлы резервными в случае отказов;

– координировать работы, необходимые для восстановления функционирования систем в прежнем или резервном помещении;

– организовать перевозки запасных частей для замены в основном помещении;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– начать работу в соответствии с графиком полной загрузки оборудования.

4.4. После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

5. Управления делами.

5.1. При обнаружении поступления воды в помещениях Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– сообщить в УИТ;

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– совместно с Группой безопасности обеспечить эвакуацию сотрудников и клиентов Банка, спасение и охрану материальных ценностей;

– в случае необходимости вызвать ремонтную техническую бригаду.

5.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– по указанию ГУЧС совместно с УИТ выделить специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями затопления;

– совместно ФАУ оценить ущерб, причиненный помещениям и имуществу Банка, составить и проанализировать список потребностей;

– уведомить поставщиков о чрезвычайной ситуации и информировать их об адресе резервного помещения;

– координировать работы по ремонту или подготовке нового постоянного помещения в первоначальном или новом месте;

– организовать перевозки и размещение персонала, материалов и оборудования в резервных помещениях;

– обеспечить энергоснабжение, подводку необходимого электрического питания, кабелей и соединителей;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования;

– обеспечить дополнительные офисные помещения мебелью и другим офисным оборудованием.

6. Управление правового обеспечения.

6.1. При обнаружении поступления воды в помещения Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– сообщить в Управление делами или в УИТ;

– выключить компьютеры и оргтехнику;

– выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– обеспечить сохранность правоустанавливающих, учредительных и регистрационных документов Банка, документов по эмиссиям Банка, протоколов заседания Наблюдательного совета, Общего собрания акционеров Банка, Комитета по проблемным активам;

– закрыть все оборудование большими пластиковыми пленками или листами, при их наличии;

– при угрозе жизни и здоровью сотрудникам Управления и посетителям, находящимся в Управлении и переговорных комнатах, эвакуироваться из занимаемых в Банке помещений маршрутом и в место, указанными Группой безопасности;

– после сообщения о ликвидации угрозы или последствий затопления возобновить деятельность на рабочих местах.

6.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

7. Все сотрудники Банка.

7.1. При обнаружении поступления воды в помещения Банка:

– сообщить на пост охране по телефонам, указанным в Приложении №4;

– сообщить в Управление делами или в УИТ;

– по согласованию с сотрудниками УИТ выключить компьютеры, работа которых некритична для работы Банка;

– выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– перенести используемые носители информации, наиболее важные документы в безопасное место;

– обеспечить сохранность конфиденциальных документов, печатей и штампов;

– закрыть все оборудование большими пластиковыми пленками или листами;

– при угрозе жизни и здоровью сотрудникам подразделений Банка и посетителям, находящимся в подразделениях и переговорных комнатах, эвакуироваться из занимаемых Банком помещений маршрутом и в место, указанными Группой безопасности;

– после сообщения о ликвидации угрозы и последствий затопления возобновить деятельность на рабочих местах.

7.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

7.3. УИТ, ОИБ СБ, Управляющий делами, сотрудники Управления делами, Управление по работе с корпоративными клиентами, Управление развития банковских услуг, Центр электронных услуг и обслуживания физических лиц, Управление «Расчетный центр»:

– осуществить мероприятия с учетом особенности выполняемых конкретным подразделением функций (согласно пунктам 1.4.2, 1.5.4, 1.8, 1.9, 1.13 Приложения №1 «А»).

Приложение №1 «Е»
к Плану ОНиВД

Порядок действий в случае чрезвычайных ситуаций природно-техногенного характера

1. Группа безопасности - Начальник Службы безопасности Банка, Начальник дежурной смены.

– Начальнику дежурной смены охраны сообщить начальнику Службы безопасности Банка и через Управление делами руководству Банка, а также руководителю арендодателя;

– организовать оповещение сотрудников Банка при помощи громкой связи, Управляющий делами организует оповещение сотрудников Банка иными доступными средствами связи;

– совместно с Управляющим делами обеспечить жизнеобеспечение сотрудников и клиентов Банка (включение-выключение кондиционеров, воздушных притоков систем вентиляции, закрытие и усиление оконных проемов и дверных входов);

– усилить охрану путем снятия наружных постов и учащенного обхода помещений и этажей, занимаемых Банком;

– в случае необходимости сообщить о чрезвычайной ситуации подразделениям пожарной охраны и МЧС по телефонам, указанным в Приложении №4;

– в случае необходимости организовать эвакуацию сотрудников и клиентов Банка, эвакуацию и охрану материальных ценностей;

– прекратить все работы в здании, кроме работ, связанных с мероприятиями по ликвидации последствий чрезвычайной ситуации и спасению сотрудников и клиентов Банка, используя для этого имеющиеся силы и средства;

– поддерживать связь с подразделениями МЧС города, района о сложившейся ситуации и положении дел;

– встретить подразделения пожарной охраны и МЧС и оказать помощь в выборе кратчайших путей доступа к зоне разрушений;

– сообщить подразделениям пожарной охраны и МЧС сведения об особенностях конструкции здания и хранящихся опасных (взрывоопасных), взрывчатых, сильнодействующих ядовитых веществах, необходимые для обеспечения безопасности личного состава.

2. Руководитель ГУЧС:

– при получении информации об угрозе стихийных бедствий или в случае непредвиденных ситуаций техногенного характера созвать Группу управления в чрезвычайных ситуациях (ГУЧС);

– принять решение о приостановлении работы и эвакуации сотрудников Банка;

– координировать обмен информацией с клиентами Банка, МГТУ Банка России и средствами массовой информации.

3. Группа управления в чрезвычайных ситуациях (ГУЧС).

3.1. При объявлении эвакуации:

– принять решение о времени возвращения сотрудников Банка на свои рабочие места.

3.2. В случае нанесения ущерба здоровью сотрудников Банка, оборудованию и помещениям, занимаемым Банком:

– определить полноту выполнения Плана ОНиВД;

– дать указание Управляющему делами о применении мобильного телефона, приобретенного и хранящегося в ОМТО УД и используемый только для осуществления передачи и получения информации, связанной с чрезвычайной ситуацией;

– регулярно информировать руководителей структурных подразделений Банка о текущей ситуации;

– принять решение о необходимости возобновления работы Банка в резервном или основном помещении Банка и дать соответствующие указания руководителям структурных подразделений Банка;

– временно освободить сотрудников Банка от работы до сообщения информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– в случае необходимости рассмотреть варианты получения сторонней профессиональной помощи от аварийных служб, поставщиков оборудования и ПО;

– корректировать график замещения должностей в зависимости от наличия и работоспособности персонала Банка;

– координировать прием на работу, для скорейшего заполнения всех недостающих вакансий;

– расследовать причины возникновения чрезвычайной ситуации.

4. УИТ.

4.1. При обнаружении угрозы возникновения природно-техногенных факторов:

– выключить компьютеры, работа которых некритична для работы Банка;

– контролировать функционирование оборудования.

Если не удается предотвратить последствия воздействия природно-техногенного фактора:

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– закрыть все оборудование большими пластиковыми пленками или листами.

– эвакуировать сотрудников Управления из занимаемых в Банке помещений маршрутом и в места, указанные Группой безопасности;

– пересчитать эвакуированных сотрудников Управления из занимаемых Банком помещений и сообщить об отсутствующих Службе безопасности Банка;

– после сообщения о ликвидации последствий непредвиденных обстоятельств природно-техногенного характера, возобновить деятельность на рабочих местах;

– в случае принятия решения ГУЧС о возобновлении работы в резервном помещении ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

4.2. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– составить график выполнения работ в резервном помещении;

– выделить совместно с Управляющим делами специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации либо принять решение о применении мобильного телефона, приобретенного и хранящегося в ОМТО УД и используемый только для осуществления передачи и получения информации;

– подготовить и оперативно подключить резервные аппаратные средства и другое оборудование;

– координировать работы, необходимые для восстановления функционирования систем в резервном помещении;

– организовать перевозки запасных частей для замены в резервном помещении;

– организовать перемещение носителей с резервными копиями в резервное помещение;

– организовать работу в резервном помещении с техническим персоналом поставщика (по мере необходимости);

– определить системную точку для восстановления с резервных копий, восстановить информацию и проверить целостность текущего состояния базы данных;

– инсталлировать в резервном помещении программное обеспечение, необходимое для возобновления основной деятельности Банка;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– совместно с пользователями подтвердить завершенность операции восстановления базы данных;

– контролировать средства обеспечения безопасности в течение процесса восстановления;

– произвести тестирование прикладных программ;

– начать работу в соответствии с графиком полной загрузки оборудования.

После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

4.3. В случае принятия решения ГУЧС о возобновлении работы в основном помещении:

– подготовить и оперативно подключить аппаратные средства и другое оборудование, восстановить функции аппаратных средств и другого оборудования АБС или оперативно заменить дефектные узлы резервными в случае отказов;

– координировать работы, необходимые для восстановления функционирования систем в прежнем или резервном помещении;

– организовать перевозки запасных частей для замены в основном помещении;

– обеспечить восстановление производственных систем, запустить системы и проверить непрерывность выполняемой обработки данных, проверить правильность процесса восстановления данных и последующей их обработки;

– начать работу в соответствии с графиком полной загрузки оборудования.

4.4. После завершения восстановления работоспособности основных компонентов АБС, её тестирования и запуска в резервном помещении:

– начать восстановление поврежденных серверных;

– настроить штатные средства защиты АБС;

– о результатах восстановления информировать ГУЧС.

5. Управление делами.

5.1. При обнаружении угрозы возникновения природно-техногенных факторов:

– совместно с сотрудниками Службы безопасности Банка обеспечить жизнеобеспечение сотрудников и клиентов Банка (включение-выключение кондиционеров, воздушных притоков систем вентиляции, закрытие и усиление оконных проемов и дверных входов);

5.2. При объявлении эвакуации:

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– закрыть все оборудование большими пластиковыми пленками или листами;

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери;

– эвакуировать сотрудников Управления из занимаемых в Банке помещений маршрутом и в место, указанным Группой безопасности;

– пересчитать эвакуированных сотрудников Управления из занимаемых в Банке помещений и сообщить об отсутствующих Группе безопасности;

– после сообщения Начальника группы безопасности о ликвидации последствий чрезвычайной ситуации возобновить деятельность на рабочих местах;

– при невозможности продолжать работу в обычном режиме ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

5.3. В случае принятия решения ГУЧС о возобновлении работы в резервном помещении:

– выделить совместно с УИТ специальный канал связи (отдельный телефонный номер (номера)), используемый только для осуществления передачи и получения информации, связанной с последствиями чрезвычайной ситуации;

– совместно с ФАУ оценить ущерб, причиненный имуществу и помещениям, занимаемым Банком, составить и проанализировать список потребностей;

– уведомить поставщиков о чрезвычайной ситуации и информировать их об адресе резервного помещения;

– координировать работы по ремонту или подготовке нового постоянного помещения в первоначальном или новом месте;

– организовать перевозки и размещение персонала, материалов и оборудования в резервных помещениях;

– обеспечить энергоснабжение, подводку необходимого электрического питания, кабелей и соединителей;

– обеспечить непрерывность функционирования сети связи;

– в случае необходимости обеспечить взаимодействие с телефонной компанией с целью полного восстановления связи и, при необходимости, замены телекоммуникационного оборудования;

– обеспечить дополнительные офисные помещения мебелью и другим офисным оборудованием.

6. Управление правового обеспечения.

6.1. При объявлении эвакуации:

Если время позволяет:

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– обеспечить сохранность правоустанавливающих, учредительных и регистрационных документов Банка, документы по эмиссиям Банка, протоколов заседания Наблюдательного совета, Общего собрания акционеров Банка, Комитета по проблемным активам;

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все оборудование большими пластиковыми пленками или листами, при их наличии;

– закрыть все двери;

– эвакуировать сотрудников Управления и посетителей, находящихся в подразделении и переговорных комнатах, из занимаемых в Банке помещений, маршрутом и в место, указанными Группой безопасности;

– пересчитать эвакуированных сотрудников Управления из занимаемых в Банке помещений и сообщить об отсутствующих Группе безопасности;

– после сообщения о ликвидации последствий чрезвычайной ситуации возобновить деятельность на рабочих местах;

– при невозможности продолжать работу в штатном режиме ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места;

– совместно с ФАУ и Службой безопасности проанализировать возникший в результате чрезвычайной ситуации ущерб и направить соответствующие претензии виновнику аварии и в страховую компанию запрос на проведение его оценки;

– обработать все поступившие заявления об ущербе;

– предоставить Руководителю ГУЧС подробный отчет об ущербе;

– подготовить требования к страховой компании о возмещении ущерба;

– обеспечить представление интересов Банка в суде и взаимодействие со Службой судебных приставов и иными государственными органами.

7. Все сотрудники Банка.

7.1. При объявлении эвакуации:

Если время позволяет:

– по согласованию с сотрудниками УИТ выключить компьютеры, работа которых некритична для работы Банка;

– перенести используемые носители информации, наиболее важные документы и ценное имущество в безопасное место;

– обеспечить сохранность конфиденциальных документов, печатей и штампов;

– закрыть все оборудование большими пластиковыми пленками или листами;

– выходя из помещения, в котором находятся компьютеры, выключить аварийные выключатели электрического питания, вентиляционные системы и кондиционеры, обесточить компьютеры и оргтехнику;

– закрыть все двери.

7.2. При невозможности продолжать работу в штатном режиме:

– ждать от ГУЧС информации о дате начала трудовой деятельности и местонахождении нового рабочего места.

7.3. УИТ, ОИБ СБ, Управляющий делами, сотрудники Управления делами, Управление по работе с корпоративными клиентами, Управление развития банковских услуг, Центр электронных услуг и обслуживания физических лиц, Управление «Расчетный центр»:

– осуществить мероприятия с учетом особенности выполняемых конкретным подразделением функций (согласно пунктам 1.4.2, 1.5.4, 1.8, 1.9, 1.13 Приложения №1 «А») в Головном офисе Банка на арендуемых площадях по адресу: _____ _____.

8. Особенности действий в случае в случае урагана:

– основными факторами, влияющими на непрерывность деятельности Банка, при урагане является частичное разрушение помещений, занимаемых Банком (выбивание окон, порча кровли), возможна порча документов, нарушение связи и отключение электропитания;

– основными опасными факторами урагана являются массивные конструкции, деревья, перемещаемые сильным ветром.

– на случай нарушения связи и отключения электропитания.

Инструкции
о действии сотрудников Банка при урагане

№	Действия	Комментарий	Исполнитель	Сроки исполнения
1	Организовать постоянное наблюдение за состоянием окружающей среды и происходящими в ней изменениями	Наблюдение может производиться с помощью средств массовой информации	Руководитель ГУЧС	Постоянно с момента объявления о возможности урагана
2	Закрыть все окна и двери, не выходить из помещений, занимаемых Банком	Сотрудникам Банка следует отойти от окон и занять безопасное место у стен внутренних помещений, в коридоре, у встроенных шкафов, в туалетных комнатах, кладовых, в прочных шкафах, под столами	Все сотрудники Банка	Немедленно

3	Провести противопожарные мероприятия, отключить все неиспользуемое оборудование, организовать контроль за состоянием всех помещений Банка (структурного подразделения Банка)		Сотрудники Банка, ОМТО УД	Немедленно
4	Проведение критических операций в чрезвычайном режиме	Критические операции производятся строго в соответствии с действующим законодательством. в случае недостатка ресурсов для осуществления таких операций сотрудники Банка действуют в соответствии с Порядком осуществления критических операций в чрезвычайном режиме, порядок доступа к ресурсам	Сотрудники соответствую-щих подразделений Банка	Постоянно

Контрольный лист руководителя ГУЧС в случае урагана:

– организовать постоянное наблюдение за состоянием окружающей среды и происходящими в ней изменениями;

– провести противопожарные мероприятия, отключить все неиспользуемое оборудование, организовать контроль за состоянием всех арендуемых Банком помещений.

План выхода из кризисной ситуации при урагане:

– по завершении урагана руководитель ГУЧС принимает решение о возобновлении работы в повседневном режиме.

Приложение №1 «Ж»
к Плану ОНиВД

Порядок действий в случае чрезвычайных ситуаций техногенного характера (отказа систем кондиционирования, отключения электропитания, разрушения баз данных, неисправности серверного оборудования)

Наим-вание группы (структурного подразделения Банка)	**Порядок действий в случае отказа систем кондиционирования**	**Порядок действий в случае отключения электропитания**	**Порядок действий в случае неисправности серверного оборудования**	**Порядок действий в случае разрушения баз данных**
УИТ	**Специалисту УИТ:** - ставит в известность Начальника УИТ; - в случае превышения температуры помещения выше 30 градусов, **Начальнику УИТ** решить, работа какого оборудования и действие каких не критичных для деятельности Банка АБС могут быть приостановлены, и сообщить об этом пользователям.	В случае отключения основного и резервного электропитания **Начальнику УИТ :** - при отказе ИБП перевести на режим pass-through и установить связь с обслуживающей организацией по указанным в Приложении №4 телефонам. - обеспечить (при содействии ОМТО УД) переключение ключевой вычислительной техники и коммуникационного оборудования на действующие розетки; - обеспечить (при содействии ОМТО УД, при наличии необходимости совместно с арендодателем) переход на резервный источник питания	**Начальнику УИТ:** - доложить о неисправности серверного оборудования Президенту Банка либо Заместителю, Президента, курирующему данное направление; - организовать восстановление работоспособности оборудования; - в случае необходимости – обеспечить перевод модулей АБС на резервные мощности; - оповестить начальника отдела ИБ; - по указанным в Приложении №4 телефонам установить связь с поставщиком оборудования (сервисным центром) и определить сроки ремонта	**Начальнику УИТ:** - доложить Президенту Банка либо Заместителю Президента, курирующему данное направление; - по указанным в Приложении №4 телефонам связаться со специалистами компании «RS-bank»; - попытаться восстановить структуру и данные с помощью специалиста компании «RS-bank»; - при необходимости восстановить данные с резервной копии; - оповестить Начальника отдела ИБ СБ.
УД	Начальнику отдела материально-технического обеспечения (ОМТС): принять срочные меры по восстановлению функций системы кондиционирования и снижения температуры помещения до необходимого уровня, оповестить арендодателя.	**Управляющему делами**: - доложить об отключении системы кондиционирования Президенту Банка; По указанным в Приложении №4 телефонам установить: - связь с Московской кабельной сетью; - обеспечить переключение ключевой вычислительной техники и коммуникационного оборудования на действующие розетки; - сообщить об отключении электропитания арендодателю и службам электросети города; - обеспечить совместно с арендодателем переход на резервный источник питания; -согласовать и контролировать порядок аварийных работ.		
Группа безопасности; Начальник СБ, Начальник дежурной смены		Начальник дежурной смены докладывает об отключении электропитания начальнику СБ Банка, ОМТС УД, а Управление делами - руководству банка; При необходимости или по указанию руководства Банка сообщить об отключении службам электросети города; По громкой связи оповестить сотрудников и клиентов Банка об отключении электропитания и времени возможного устранения неисправности; (оповещение возможно только в течение 30 минут после отключения электричества); В дальнейшем действовать по указанию руководства Банка и Начальника СБ Банка.		
Управление	Работа по досудебному	Работа по досудебному	Работа по досудебному	Работа по досудебному

правового обеспечения (УПО)	урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств
ФАУ	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка
Сотрудники Банка	В случае превышения температуры помещения выше 25 градусов, уведомить ответственного специалиста УИТ. Если средства вычислительной техники выключены по указанию Начальника УИТ или они отключаются сами из-за чрезмерного перегрева, не включать их до снижения температуры помещения до необходимого уровня.	Действовать согласно указаниям руководства и Начальника СБ Банка.	Уведомить ответственного специалиста УИТ о нарушении нормального режима работы оборудования.	Уведомить ответственного специалиста УИТ о прекращении доступа к базам данных.

Приложение №1 «З»
к Плану ОНиВД

Порядок действий в случае прекращения доступа в Интернет и нарушения функционирования систем связи

Наимен-ние группы (структур-го подразд-ния Банка)	**Порядок действий в случае прекращения доступа в Интернет**	**Порядок действий в случае неисправности системы «I-bank», «Клиент-Банк»**	**Порядок действий в случае неисправности системы Telex**	**Порядок действий в случае неисправности системы S.W.I.F.T.**	**Порядок действий в случае неисправности торговых систем ММВБ**
УИТ	В случае прекращения доступа в Интернет через одного из провайдеров Начальнику УИТ: - доложить о прекращении доступа в Интернет Президенту Банка либо Заместителю Президента, курирующему данное направление и Управляющему делами для информирования сотрудников; - обратиться к провайдеру относительно характера отказа и сроков восстановления работоспособности; - переключить оборудование на работу с исправным каналом.	Начальнику УИТ, в случае неисправности систем «I-bank», «Клиент-Банк» доложить о неисправности Президенту Банка либо Заместителю Президента, курирующему данное направление; курирующему Вице-президенту; Начальнику отдела ИБ СБ. Начальнику Отдела расчетных систем и банковских телекоммуникаций: - проверить каналы связи; - установить связь с производителем программного обеспечения; - осуществить проверку оборудования; - развернуть систему на резервных мощностях	Начальнику УИТ: - доложить о неисправности Президенту Банка либо Заместителю Президента, курирующему данное направление; - проверить работоспособность оборудования; - обратиться в бюро ремонта	Начальнику Отдела расчетных систем и банковских телекоммуникаций - Доложить начальнику УИТ: - доложить о неисправности Президенту Банка либо Заместителю Президента, курирующему данное направление и/или курирующему Вице-президенту; -установить связь с провайдером и организатором доступа к системе; - в случае необходимости – переключить на резервный сервер	Начальнику УИТ, Начальнику Казначейства: - доложить о неисправности Президенту Банка либо Заместителю Президента, курирующему данное направление; - проверить каналы связи; - обратиться в технический центр ММВБ.
Управление правового обеспечения (УПО)	Работа по досудебному урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	Работа по досудебному урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	Работа по досудебному урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств	Работа по досудебному урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств:	Работа по досудебному урегулированию вопроса взыскания ущерба. Обеспечение представления интересов Банка в суде в случае судебных разбирательств
ФАУ	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка	Оценка влияния непредвиденных обстоятельств и понесенного в результате их воздействия ущерба на показатели деятельности Банка
Сотрудники Банка	Уведомить ответственного специалиста УИТ о прекращении доступа в Интернет.	Уведомить ответственного специалиста УИТ о прекращении доступа в Интернет и жалобах клиентов.	Уведомить ответственного специалиста УИТ о прекращении функционирования системы Telex.	Уведомить ответственного специалиста УИТ о прекращении функционирования системы S.W.I.F.T.	Уведомить ответственного специалиста УИТ о неисправности торговой системы ММВБ.

Приложение №1 «И»
к Плану ОНиВД

Порядок действий в случае кризиса ликвидности

Банк действует в соответствии с «Положением по управлению и контролю ликвидностью и риском ликвидности», утвержденным Наблюдательным советом (Протокол от 04.02.2015 №8/2015).

Объектами риска ликвидности являются входящие и исходящие потоки платежей Банка, распределенные по срокам их осуществления. Риск ликвидности возникает тогда, когда в день осуществления платежей объем исходящих платежей превышает объем входящих, и для покрытия образовавшегося разрыва, называемого дефицитом ликвидности, Банк должен выполнить мероприятия обеспечения ликвидности.

1. Перечень превентивных мер, выполнение которых в режиме повседневного функционирования Банка необходимо для поддержания ликвидности.

Мероприятия	**Ответственное подразделение**	**Орган управления, оперативные комитеты**
Анализ срочной структуры баланса Банка, выявление возможных угроз ликвидности, разработка предложений по оптимизации структуры и их осуществление	ФАУ, Казначейство	Правление Банка, Финансовый комитет
Анализ условий договоров с основными организациями-контрагентами, оценка правовых, репутационных рисков в условиях возникновения непредвиденных обстоятельств	Управление правового обеспечения (УПО)	
Определение контрагентов по договорам финансовой помощи на случай непредвиденных обстоятельств. Проработка условий и заключение договоров финансовой помощи на случай непредвиденных обстоятельств	Казначейство, УПО	Президент Банка, Правление Банка, Наблюдательный совет
Разработка коммуникационных мероприятий и определение информационного обеспечения на случай прямой угрозы потери деловой репутации. Разработка правил и процедур распределения ответственности и полномочий между руководителями и структурными подразделениями Банка в условиях чрезвычайной ситуации	Управление делами, УПО	Правление Банка, Финансовый комитет, ГУЧС
Разработка порядка действий и инструкций для руководителей и сотрудников структурных подразделений Банка в случае возникновения непредвиденного дефицита ликвидности	Казначейство, ФАУ, УПО	Правление Банка, Финансовый комитет, ГУЧС
Системное внесение изменений во внутренние нормативные документы (Устав, Положение о системе внутреннего контроля, Положение о Службе внутреннего контроля, Политики, Положения о подразделениях, должностные инструкции и иные внутренние документы Банка).	УПО, СВК, руководители структурных подразделений Банка	Правление Банка, Наблюдательный совет

Синхронизация существующей нормативной базы с учетом разработанных и переработанных документов, проведение проверок действия Плана ОНиВД	УПО, СВК, руководители структурных подразделений Банка	Правление Банка, Наблюдательный совет, ГУЧС

2. Источники погашения дефицита ликвидности

Источники погашения дефицита ликвидности	**Методы уменьшения дефицита ликвидности**	**Координатор от руководящего состава Банка**	**Ответственное подразделение / Комитет**
Установление обширных корреспондентских отношений	Заключение новых корреспондентских отношений	Президент Банка, Курирующий Вице-президент	Управление «Расчетный центр», Отдел корреспондент. отношений и международных расчетов
Межбанковские кредиты	- наличие необходимого объема средств в качестве залога; - заключение новых договоров МБК; - расширение списка контрагентов	Президент Банка, в его отсутствие – Заместитель Президента Банка	Кредитный комитет, Казначейство
Рефинансирование Банка России	- поддержание необходимого количества ценных бумаг, свободных от залога; - приобретение ценных бумаг, входящих в ломбардный список Банка России	Президент Банка, в его отсутствие – Заместитель Президента Банка	Кредитный комитет, Казначейство
Увеличение собственных долговых обязательств (собственные векселя)	- работа с клиентами, находящимися на расчетно-кассовом обслуживании; - расширение клиентской базы	Президент Банка, в его отсутствие – Заместитель Президента Банка	Казначейство, Управление по работе с корпоративными клиентами, Управления развития банковских услуг
Привлечение субординированного кредита	Привлечение долгосрочных средств акционеров и внешних инвесторов	Президент Банка, в его отсутствие – Заместитель Президента Банка	Управление правового обеспечения, Финансовый комитет
Увеличение уставного капитала	Эмиссия ценных бумаг Банка	Президент Банка, в его отсутствие – Заместитель Президента Банка	Управление правового обеспечения, Финансовый комитет,

3. Методы мобилизации активов

Активы	**Методы мобилизации активов**	**Координатор от руководящего состава Банка**	**Подразделение, отвечающее за операции / Комитет**
Просроченные кредиты	- активные усилия Банка, направленные на получение средств по долгам; - изменение графика обслуживания обязательств по долгу;	(КПА) Комитет по проблемным активам, Вице-президент, курирующий	Кредитное-финансовое управление, Кредитный комитет, КПА

	- получение дополнительного или существенного залогового обеспечения долговых обязательств; - продажа просроченных активов на свободном рынке долговых обязательств	Кредитное-финансовое управление	
Межбанковские кредиты	- изменение графика возвратов кредитов, там, где это возможно, с досрочным возвратом	Руководитель Казначейства	Кредитный комитет, Казначейство
Ценные бумаги	продажа государственных ценных бумаг, продажа акций, продажа векселей, продажа облигаций	Руководитель Казначейства	Кредитный комитет Казначейство,
Резервы Банка	- формирование резервов на возможные потери по ссудам и резервов под сомнительные активы	Главный бухгалтер Банка, Начальник Службы внутреннего контроля	Управление учета и налоговой отчетности, Управление сводной отчетности, Кредитный комитет, СВК

4. Мероприятия по управлению активами

Мероприятия	**Ответственное подразделение**	**Орган управления, оперативные комитеты**
Касса:	Управление «Расчетный центр», Центр электронных услуг и обслуживания физических лиц, Управление развития банковских услуг, обособленные структурные подразделения Банка	ГУЧС, Финансовый комитет
- установление лимитов кассовой наличности (по объемам или по оборачиваемости);		
- ежедневное информирование руководителя структурного подразделения Банка (на основе 3-х дневного прогноза);		
- контроль за обязательной ежедневной инкассацией остатков наличности (остающейся в кассе после выплат наличных клиентам) на корреспондентский счет в Банке России.		
Средства на корреспондентских счетах в Банке России и иных кредитных организациях, НКО, Банках-нерезидентах:		
- установление очередности платежей по их важности (с учетом первоочередности клиентских платежей и необходимости поддержания текущей деятельности Банка).	Казначейство, Управление «Расчетный центр», Центр электронных услуг и обслуживания физических лиц, Управление развития банковских услуг, обособленные структурные подразделения Банка	ГУЧС, Курирующие вице-президенты и заместители Президента Банка
Межбанковское кредитование и корреспондентские счета «ностро» в	Казначейство, Центр электронных услуг и	ГУЧС, Финансовый

банках-резидентах РФ:	обслуживания физических лиц, Управление «Расчетный центр»	комитет, Кредитный комитет
- ужесточение лимитов на операции с банками-контрагентами (снижение, фиксирование, закрытие);		
- сокращение обязательств по заключенным ранее кредитным линиям по кредитованию других банков;		
- хеджирование проводимых Банком операций в зависимости от конкретной ситуации (встречные сделки, сделки с покрытием и т.п.).		
Кредитный портфель:	КФУ, УПО, Управление «Расчетный центр», Центр электронных услуг и обслуживания физических лиц, Управление развития банковских услуг, обособленные структурные подразделения Банка	ГУЧС, Финансовый комитет, Кредитный комитет, Правление Банка
- принятие мер по досрочному возврату части кредита;		
- рассмотрение возможности реализации части кредитного портфеля другим банкам;		
- ужесточение лимитов (снижение, фиксирование, закрытие); пересмотр сроков выдаваемых кредитов в сторону коротких;		
- рассмотрение возможности перераспределения полномочий между обособленными структурными подразделениями Банка и Головным офисом Банка: введение полной или частичной централизации функций кредитования;		
- определение возможности повышения процентных ставок, пересмотр тарифной политики;		
определение перечня клиентов, кредитование которых не должно прекращаться.		
Портфель ценных бумаг:	Казначейство	ГУЧС, Финансовый комитет, Кредитный комитет, Правление Банка
- рассмотрение возможности реализации части портфеля ценных бумаг;		
- ужесточение лимитов (снижение, фиксирование, закрытие);		
- реструктуризация портфеля ценных бумаг в направлении сокращения его сроков.		
Основные средства и капитальные вложения:	Управление делами, ФАУ	Президент Банка, Финансовый комитет
- рассмотрение возможности ограничения наращивания основных средств и капитальных вложений и других неоперационных расходов;		
- установление запрета, установление		

ограничивающего размера наращивания основных средств и капитальных вложений, и других неоперационных расходов;		
- рассмотрение возможности реализации части основных средств.		

5. Основные мероприятия по управлению пассивами

Мероприятия	**Ответственное подразделение**	**Орган управления, оперативные комитеты**
Межбанковские займы:	Казначейство, ФАУ	Финансовый комитет
- увеличение объемов и/или продление срока погашения межбанковских депозитов;		
- активизация работы по использованию ранее заключенных кредитных линий по привлечению средств других кредитных организаций;		
- регулярный анализ наличия и объемов концентрированных привлеченных средств от одного держателя;		
- оперативное приобретение средств (в т.ч. заимствований на внешних финансовых рынках);		
- привлечение займов по сделкам «РЕПО», под залог ценных бумаг, основных фондов.		
Клиентские счета:	Управление «Расчетный центр», Центр электронных услуг и обслуживания физических лиц, обособленные структурные подразделения Банка, Управление развития банковских услуг	Финансовый комитет, Правление Банка
- рассмотрение и оценка возможности внедрения более привлекательных услуг и условий по расчетно-кассовому обслуживанию клиентов Банка в целях заинтересованности клиентов в сохранении остатков на счетах в Банке;		
- регулярный анализ наличия и объемов концентрированных привлеченных средств от одного держателя.		
Депозиты:	Управление «Расчетный центр», Центр электронных услуг и обслуживания физических лиц, Управление развития банковских услуг, обособленные структурные подразделения Банка, Казначейство	Финансовый комитет, Президент Банка, Правление Банка
- выработка новых продуктов по дополнительному привлечению депозитных средств;		
- изменение процентных ставок;		
- варьирование сроков в сторону удлинения сроков размещения депозитных средств;		
- регулярный анализ наличия и объемов концентрированных привлеченных средств от		

одного держателя.		
Субординированные займы (кредиты)	УПО, ФАУ	Правление Банка, Президент Банка, Наблюдательный совет
Финансовая помощь или депозиты (займы) акционеров	УПО	Правление Банка, Президент Банка, Наблюдательный совет

ГУЧС, Финансовый комитет:

Принять решение:

– о стратегии ликвидации кризиса ликвидности;

– о возможных путях ликвидации кризиса ликвидности.

ФАУ:

Провести:

– оценку размера риска потери ликвидности;

– оценку структуры активов и пассивов по объемам и срокам погашения;

– оценку оттока ресурсов из Банка на ближайшие 3 месяца;

Финансовый комитет, Уполномоченные внутренние подразделения:

Реструктуризировать активы:

– продажа портфеля облигаций;

– привлечение краткосрочных кредитов (депозитов) от коммерческих банков, в соответствии с открытыми на Банк лимитами;

– провести переговоры с крупнейшими клиентами и контрагентами, в целях снижения значительного оттока средств;

– ограничить (прекратить) кредитование на определенный срок, ограничить другие активные операции;

– привлечь долгосрочные кредиты (депозиты);

– получить субординированные займы (кредиты);

– реструктуризировать обязательства, например, депозиты (вкладов), в т. ч. принадлежащие акционерам (участникам) и сотрудникам Банка, из краткосрочных в долгосрочные обязательства и/или субординированные кредиты/депозиты;

– сократить либо приостановить проведение расходов, в том числе управленческих, включая (частично) заработную плату сотрудников Банка;

– контроль со стороны СВК с периодичностью не реже 1 раза в две недели за реализацией мероприятий по восстановлению ликвидности и/или исполнения включенных в него процедур;

– ежедневно информировать Финансовый комитет и Правление Банка о ходе ликвидации потери ликвидности.

Управление правового обеспечения:

– обеспечить юридическое сопровождение всех поступивших претензий и исков от пострадавших клиентов Банка;

– обеспечить представление интересов Банка в судебных органах.

Приложение №1 «К»
к Плану ОНиВД

Порядок действий в случае массовых беспорядков

1. Основными факторами, влияющими на непрерывность деятельности Банка, при массовых беспорядках является возможная порча имущества Банка (оборудования) (см. Порядок действий в случае нападения на персонал и собственность Банка).

2. Основным опасным фактором массовых беспорядков являются неадекватные действия толпы. Возможно возгорание (см. Порядок действий в случае пожарной тревоги).

3. Особенности осуществления Плана ОНиВД в случае массовых беспорядков в Головном офисе Банка на арендуемых площадях по адресу: _____.

№	Действия	Комментарий	Исполнитель	Сроки исполнения
1	Организовать постоянное наблюдение за происходящими событиями	Наблюдение может производиться с помощью средств массовой информации	Начальник Службы безопасности Банка, Начальник дежурной смены, Руководитель ГУЧС	Постоянно с момента объявления о возможности массовых беспорядков в районе месторасположения Банка
2	Закрыть все окна и двери, не выходить из помещений, занимаемых Банком убрать важные документы	Сотрудникам Банка следует отойти от окон и занять безопасное место у стен внутренних помещений, в коридоре; убедиться, что важные документы не находятся в зоне поражения	Все сотрудники Банка	Немедленно
3	Провести противопожарные мероприятия, отключить все неиспользуемое оборудование, организовать контроль за состоянием всех помещений, занимаемых Банком		Ответственный сотрудник арендодателя, отвечающий за пожарную безопасность и ответственные за пожарную безопасность сотрудники Банка в помещении	Немедленно
4	Оповещение заинтересованных лиц	Принятие решения по организации оповещения	Руководитель ГУЧС	Немедленно
5	Проведение критических операций в чрезвычайном режиме	Критические операции производятся строго в соответствии с действующим законодательством, в случае недостатка ресурсов для осуществления таких операций сотрудники Банка действуют в соответствии с Порядком осуществления критических операций в чрезвычайном режиме, порядок доступа к ресурсам	Сотрудники соответствующих структурных подразделений Банка	Постоянно

План выхода из кризисной ситуации в случае массовых беспорядков:

– участники ГУЧС оценивают возможность продолжения проведения основных операций в основном помещении в полном (сокращенном) объеме;

– в случае если помещение пострадало несущественно и продолжение всех операций возможно в основном помещении, руководитель ГУЧС принимает решение о прекращении работы в чрезвычайном режиме и переходе в обычный режим работы. Решение оформляется приказом руководителя ГУЧС;

– в случае если имеется возможность проводить основные операции в сокращенном режиме, то руководитель ГУЧС принимает решение о проведении операций в сокращенном режиме (указывается, в чем именно заключается сокращенный режим) и восстановлении помещений Банка. По завершении восстановления помещений руководитель ГУЧС принимает решение прекращении работы в чрезвычайном режиме и переходе в обычный режим работы. Решение оформляется приказом;

– в случае если основное помещение Банка пострадало существенно и продолжение работы в нем невозможно, руководитель ГУЧС принимает решение о немедленном переносе проведения критических операций в резервном помещении и восстановлении основных помещений. По мере проведения восстановительных работ проведение критических операций переносится в основные помещения Банка.

При полном восстановлении всех процессов ГУЧС принимает решение о завершении работы в кризисном режиме приказом руководителя ГУЧС;

– во втором и третьем случае заинтересованные стороны оповещаются о принятом решении в порядке, изложенном выше;

– по окончании массовых беспорядков руководитель ГУЧС принимает решение о прекращении работы Банка в кризисных условиях.

УПО совместно с ФАУ

– проанализировать возникший в результате нападения ущерб;

– обработать все поступившие заявления об ущербе;

– предоставить Руководителю ГУЧС подробный отчет об ущербе;

– осуществить взаимодействие с правоохранительными органами;

– УПО обеспечить представление интересов Банка в суде.

Приложение №1 «Л»
к Плану ОНиВД

Порядок действий в случае перехода на использование резервного комплекта программно-аппаратного комплекса по взаимодействию с Платежной системой Банка России

1. Начальник Отдела расчетных систем и банковских телекоммуникаций Управления «Расчетный центр» или лицо его замещающее распределяет между сотрудниками отдела задачи по устранению сбоя и по текущей работе отдела.

2. Перечень осуществляемых действий по устранению сбоя и по текущей работе отдела:

2.1. Включить компьютер с резервным комплектом программно-аппаратного комплекса по взаимодействию с Платежной системой Банка России.

2.2. При работе с СКЗИ «Сигнатура» для шифрования данных использовать соответствующий ключевой носитель.

2.3. В случае неработоспособности основного канала связи с Платежной системой Банка России, в целях обмена платежной информацией установить соединение по резервному выделенному каналу связи или модему Dial up.

2.4. Загрузить транспортную программу УТА в соответствующей конфигурации.

2.5. Загрузить АРМ КБР и АРМ ПУР установив текущий операционный день.

2.6. При отправке платежной информации проверить в ручном режиме корректность поступления на вход программ АРМ КБР или АРМ ПУР соответствующего файла с платежной информацией, только после этого установить соединение в УТА.

2.7. Сообщить о причинах перехода (неисправность или выход из строя аппаратного и программного обеспечения, специального программного обеспечения, каналов связи и т.д.) в Управление информационных технологий и Отдел информационной безопасности Службы безопасности. Обеспечить доступ сотрудников данных подразделений в Отдел расчетных систем и банковских телекоммуникаций Управления «Расчетный центр».

2.8. Сообщить о переходе на резервный комплект и причинах перехода Начальнику Управления «Расчетный центр» и курирующему Вице-президенту.

2.9. Подготовить платежную информацию на внешнем носителе (USB Flash Drive) и сопроводительные документы для доставки уполномоченным лицом Банка в Межрегиональный центр обработки информации Банка России (далее – МЦОИ Банка России). Решение о направлении уполномоченного лица Банка в МЦОИ Банка России принимает сотрудник Банка в должности не ниже Вице-президента на основании докладов руководителей структурных подразделений Банка, участвующих в процессе отправки платежной информации и в восстановительных работах. Вице-президент информирует Президента Банка / Заместителя Президента Банка о необходимости направления сотрудника Банка в МЦОИ Банка России

2.10. После восстановления работы основного канала связи и/или компьютера с основным комплектом программно-аппаратного комплекса по взаимодействию с Платежной системой Банка России отключить резервный компьютер и возобновить работу с основным компьютером и/или каналом связи.

2.11. В целях принятия решения по информированию Службы внутреннего контроля Банка и иные заинтересованные стороны в рамках функционирования Банка, как Расчетного центра «Мультисервисной платежной системы» о риске наступления событий, угрожающих бесперебойному функционированию программно-аппаратного комплекса и каналов связи с Платежной системой Банка России, составить отчет о выполненных в хронологическом порядке действиях в соответствии с настоящей Технологической картой. Отчет предоставить Начальнику Управления «Расчетный центр» и курирующему Вице-президенту.

Приложение №1 «М»
к Плану ОНиВД

Порядок действий ответственных структурных подразделений Банка при возникновении нестандартных и чрезвычайных ситуаций

Нестандартные и чрезвычайные ситуации		**Характер угрозы**	**Действия**	**Время реагирования**	**Ответственный**
Вид	**Ситуации**				
1	2	3	4	5	6
Предпринимательский	Промышленный шпионаж	минимальная	Определяются Руководителем ГУЧС	Опционально	Назначается Руководителем ГУЧС
	Переезд Банка в другое помещение или офис	минимальная	Процесс переезда структурных подразделений Банка планируется заблаговременно и проводится поэтапно без остановки процессов. Непрерывность процесса обеспечивается руководителем переезжающего структурного подразделения Банка	Опционально	Управление делами. ОМТО УД
	Слияние Банка с другими банками или приобретение других банков	минимальная	Данные вопросы предварительно прорабатываются с УПО	Опционально	Начальник Управления правового обеспечения
	Негативная информация о Банке в прессе	средняя	В случае появления негативной информации о Банке в прессе сотрудник Отдела связей с общественностью и рекламы Банка связывается со СМИ, опубликовавшими данную информацию, и проводит работу по публикации опровержения / изложению достоверных фактов	Опционально	Управляющий делами
1	2	3	4	5	6

Человеческий	Отсутствие планирования замещения должностей	средняя	Выделение ключевых должностей, оценка потенциального риска ухода сотрудника с данной должности, а также планирование преемников и их подготовка и развитие к занятию ключевой должности или удержание высокоэффективных и обладающих потенциалом развития преемников	Опционально	Отдел по работе с персоналом
	Несчастный случай на рабочем месте, повлекший за собой гибель сотрудника (в т.ч. в результате суицида)	минимальная	Сообщить ответственным сотрудникам	Опционально	
Техногенный	Атаки хакеров и крэкеров	серьезная	Ограничение и разграничение доступа сотрудников Банка к электронным ресурсам, в том числе к Интернет- ресурсам. Организация антивирусной защиты. Установка и настройка межсетевых экранов. Ограничение на прием на корпоративную электронную почту подозрительных Интернет сообщений. Выполнение мероприятий, предусмотренных	Опционально	Отдел информационной безопасности Службы безопасности Банка
1	2	3	4	5	6

			внутренними документами Банка в области информационной безопасности, в т.ч. периодическое тестирование на проникновение и принятие мер обеспечения безопасности. Выполнение мероприятий по защите от ДДОС атак.		
	Компьютерные вирусы	серьезная	Использование программ антивирусной защиты, их своевременная актуализация. Ограничение доступа сотрудников Банка к Интернет- ресурсам, которые потенциально несут угрозу Распространения компьютерных вирусов. Ограничение на прием на корпоративную электронную почту подозрительных Интернет сообщений	Опционально	Отдел информационной безопасности Службы безопасности Банка
	Нарушения работы общественного Транспорта	минимальная	Определяются Начальником ОМТО УД	Опционально	Начальник ОМТО УД
Природный	Снежная буря	средняя	Вызываются профильные аварийно-спасательные службы города и своими силами и имеющейся уборочной техникой боремся с последствиями стихий	Опционально	Начальник ОМТО УД
1	2	3	4	5	6

	Землетрясение	минимальная	Вызываются спасательно-аварийные службы, своими силами предпринять все возможные действия для минимизации ущерба для Банка и здоровья сотрудников Банка	Опционально	Начальник ОМТО УД
	Электромагнитные бури	минимальная	Определяются Руководителем ГУЧС	Опционально	Назначается Руководителем ГУЧС
Природно-техногенный	Падение искусственных и природных объектов с неба	минимальная	Определяются Руководителем ГУЧС	Опционально	Назначается Руководителем ГУЧС

Приложение №2
к Плану ОНиВД

Порядок поддержания непрерывности деятельности в области информационных технологий и информационной безопасности

1. Обеспечение информационной безопасности осуществляется в соответствии с внутренними документами Банка, разработанными и утвержденными в соответствии с принятыми регламентами. Основным документом является Корпоративная политика информационной безопасности, в которой определены направления работы по обеспечению информационной безопасности.

1.1. Управление доступом к информационным активам и регистрация регламентируются внутренним документом Банка – Частной политикой по управлению доступом к информационным ресурсам.

1.2. Антивирусная защита автоматизированных банковских систем и других существенно значимых данных в компьютерной сети Банка регламентируются Частной политикой по обеспечению антивирусной защиты, в которой отражены последовательности действий всех участников процесса антивирусной защиты информации, в случае обнаружения вируса или подозрения на таковое.

1.3. Установление стандарта для создания паролей, их защиты от компрометации и регулярной смене регламентируется Частной политикой парольной защиты.

1.4. Модель угроз и потенциального нарушителя для объектов обеспечения информационной безопасности отражена во внутреннем документе Банка «Модель угроз и нарушителя безопасности информации при ее обработке в информационных системах».

1.5. Регламент управления инцидентами информационной безопасности, определение процедуры обработки инцидентов (порядок действий сотрудников Банка при обнаружении нетипичных событий (инцидентов), порядок регистрации и расследования инцидентов, выявление предпосылок их возникновения для минимизации негативных последствий, а также предотвращения их повторения возникновения регламентируется внутренним документом Банка – Частная политика по менеджменту информационной безопасности.

1.6. Обработка запросов персональных данных субъекта персональных данных или его законного представителя при обращении уполномоченного органа по защите прав субъектов персональных данных (на подтверждение наличия, ознакомление, уточнение, уничтожение или отзыв согласия на обработку персональных данных, а также на устранение нарушений законодательства, допущенных при обработке персональных данных) регламентируется такими внутренними документом Банка как:

– Политика в отношении организации обработки и обеспечения безопасности персональных данных;

– Политика защиты конфиденциальной информации от утечек по каналам связи;

– Положение об организации обработки персональных данных;

– Положение о порядке обработки персональных данных с использованием средств автоматизации;

– Положение о порядке обработки персональных данных без использования средств автоматизации;

– Правила взаимодействия с субъектами персональных данных;

– Правила обмена информацией, содержащей персональные данные, с третьими лицами и неопределенным кругом лиц.

1.7. Систематизации действий и процедур, направленных на обучение персонала вопросам информационной безопасности, регламентируется Частной политикой по обеспечению информационной безопасности при работе с сотрудниками Банка.

1.8. Порядок обращения с шифровальными средствами (средствами криптографической защиты информации (СКЗИ) регламентируется внутренними документами Банка:

– Порядок учета, хранения и использования носителей секретных ключей кода аутенизации и ключей шифрования;

– Инструкция по обращению с сертифицированными ФСБ России шифровальными средствами (средствами криптологической защиты информации).

1.9. Безопасность в среде Интернет регламентируются Частной политикой по использованию ресурсов сети Интернет и электронной почты.

1.10. Защита банковских платежных и информационных технологических процессов Банка регламентируются Частной политикой по обеспечению информационной безопасности банковских платежных технологических процессов.

2. Резервное копирование информации.

2.1. Основными средствами обеспечения непрерывной работы и восстановления автоматизированных банковских систем и других существенно значимых данных в компьютерной сети Банка являются средства ежедневного дублирования ресурсов и резервного копирования.

2.2. Порядок резервного копирования информации определяется Частной политикой резервного копирования и восстановления данных.

2.3. Для хранения резервных копий критичной информации, баз данных, исходных текстов, системной и пользовательской документации в Банке используются магнитные ленты, дисковые носители и внешние накопители, которые хранятся вне серверных помещений с обеспечением мер безопасности. Порядок хранения накопителей с резервируемой информацией определяется указанной ранее Частной политикой.

2.4. Документы Банка на бумажных носителях хранятся в нескольких экземплярах, один из которых хранится в удаленном архиве Банка.

2.5. В случае необходимости восстановления запасов специфических бланков и целях сокращения времени выставления требования к поставщику, Банк имеет образцы бланков и спецификаций для обеспечения поставщиков оригинал-макетами бланков, и ведет список поставщиков специальных бланков.

3. Резервные аппаратные средства.

Порядок восстановления автоматизированных банковских систем и других существенно значимых данных в компьютерной сети Банка регламентирован Частной политикой по использованию корпоративной ЛВС и Частной политикой по обеспечению информационной безопасности при эксплуатации информационных систем.

4. Резервный вычислительный центр (РВЦ).

4.1. Основные требования к РВЦ:

– РВЦ, каналы связи ОВЦ и РВЦ, а также имеющиеся в составе ОВЦ и РВЦ программно-аппаратные средства и персонал в случае аварийных ситуаций с высшей степенью угрозы безопасности, обеспечивают возможность оперативного перевода процесса обработки информации из ОВЦ в РВЦ в течение часа.

4.2. Аппаратно-программные средства РВЦ соответствуют следующим требованиям:

4.2.1. В РВЦ должен быть развернут минимально необходимый для организации основных бизнес-процессов Банка состав оборудования и те же версии основного и дополнительного программного обеспечения, что и в основном вычислительном центре АБС.

4.2.2. РВЦ соединен основными и резервными каналами связи с ОВЦ. Данные каналы должны быть защищены от несанкционированного доступа с помощью используемых в Банке штатных средств защиты.

4.2.3. Требования к помещениям для размещения РВЦ (по электропитанию, системам кондиционирования и другим системам жизнеобеспечения) соответствуют требованиям к ОВЦ.

4.2.4. Порядок доступа к программно-аппаратным средствам РВЦ аналогичен порядку, существующему для ОВЦ.

5. Обязанности персонала РВЦ:

5.1. Администрирование, техническое обслуживание РВЦ, включая процедуры резервного копирования и восстановления программ и данных, осуществляется в порядке, определенном для ОВЦ, силами сотрудников соответствующего структурного подразделения Банка.

5.2. Персонал РВЦ в случае аварийной ситуации по распоряжению Руководства Банка, переводит в РВЦ процесс обработки информации и обеспечивает его сопровождение вплоть до момента возвращения обработки информации в восстановленный ОВЦ.

5.3. В обязанности персонала, уполномоченного на обслуживание РВЦ, входит:

– периодическая проверка состояния аппаратно-программных средств и другого оборудования РВЦ, поддержание их в рабочем состоянии;

– восстановление функций аппаратных средств и другого оборудования РВЦ или оперативная замена дефектных узлов резервными в случае отказов.

6. Кондиционирование воздуха.

6.1. Температура помещения, в котором находятся компьютеры, не должна превышать 25 градусов.

6.2. В каждой серверной находятся датчики температуры и влажности, которые работают круглосуточно. Температура контролируется ответственным сотрудником УИТ на регулярной основе. В случае выхода из строя системы мониторинга серверных, температура проверяется по показаниям термометров.

7. Противопожарная защита.

7.1. В целях противопожарной защиты и сокращения времени реагирования на обнаружение задымленности или очага возгорания охрана Банка (в соответствии с Договором на оказание охранных услуг) обеспечена:

– схемами эвакуации сотрудников и клиентов Банка;

– первичными средствами пожаротушения (огнетушителями);

– отдельным городским телефоном и средствами оперативной связи;

– охранно-пожарной сигнализацией с выводом на Пульт централизованного наблюдения.

8. Противорадиационная защита.

8.1. Для работы с денежными знаками с радиоактивным загрязнением оборудована комната в подвальном помещении Банка.

8.2. Работа с денежными знаками с радиационным загрязнением производится с использованием средств индивидуальной защиты.

9. Система безопасности.

9.1. Помещения Банка категорируются в зависимости от критичности размещаемых в них информационных активов.

9.2. В соответствии с категорией обеспечивается техническая укрепленность помещений, оснащение средствами видеоконтроля, контроля доступа, пожаротушения и сигнализации.

9.3. В целях безопасности охрана Банка обеспечена:

– схемами эвакуации сотрудников и клиентов Банка;

– пеналами для хранения ключей от помещений и личных мастичных печатей у ответственных лиц;

– первичными средствами пожаротушения (огнетушителями);

– отдельным городским телефоном и средствами оперативной связи;

– охранно-пожарной сигнализацией с выводом на Пульт централизованного наблюдения.

10. Средства связи.

10.1. УИТ поддерживает актуальным список всего специального программного обеспечения.

10.2. УИТ и Управление делами поддерживают актуальным список поставщиков средств связи.

11. Поставщики типографских бланков, штампов и печатей.

11.1. Управление делами поддерживает актуальным список поставщиков типографских бланков, печатей и штампов.

Пример Параметров оценки критичности автоматизированных банковских систем и других существенно значимых данных в компьютерной сети Банка

Показатель		Баллы
1. Достижение среднего уровня производительности		
Количество часов после аварии	4 - 6 часов	5
	7 - 12 часов	4
	13 - 24 часа	3
	25 - 48 часов	2
	Без ограничений по времени восстановления	0
2. Потребность в особых ресурсах		
Восстановление в достаточном объеме возможно только при восстановлении специальной базы данных и/или программной/аппаратной части и/или средств связи по некоммутируемым линиям		5
Возможно функционирование в достаточной мере при использовании связи по коммутируемым линиям, если есть все необходимые ресурсы		4
Достаточная степень производительности может быть обеспечена при частичном восстановлении ключевых ресурсов (например, при использовании текущей/резервной версии базы данных)		3
Для восстановления не нужно никаких уникальных ресурсов		2
Может функционировать в течение периода после аварийного восстановления даже при отсутствии отдельных блоков и подсистем		0
3. Переносимость		
Восстановление возможно только на основном рабочем компьютере		5
Возможно перемещение на другой компьютер, но это будет достигнуто с задержкой		3
Перемещение на другой компьютер не вызовет никаких трудностей		0
4. Необходимая квалификация		
Сотрудники не смогли успешно протестировать процесс восстановления		5
Тестирование восстановления было успешным, но было достигнуто с большой задержкой		3
Тестирование восстановления прошло успешно. Не было встречено никаких проблем.		0
5. Устойчивость к потерям		
Задержка с восстановлением, скорее всего, приведет к финансовым потерям		5
Задержка с восстановлением вызовет проблемы с клиентами, вследствие чего будут превышены установленные лимиты на показатели операционного и функционального рисков		4
Задержка с восстановлением вызовет проблемы с клиентами, но в пределах установленных лимитов на показатели операционного и функционального рисков		2
При задержанном или неполном восстановлении никаких проблем не предвидится		0
6. Рабочие неисправности		
Успешное восстановление и «нормальная» эксплуатация требуют непосредственного участия ведущих специалистов УИТ		5
Имеется необходимость в текущей документации и/или был запланирован «ремонт»		4
Имеется значительная чувствительность к изменениям в объемах входных данных, их смешению и/или качеству и/или очевидная и значительная степень риска отказа в работе		3
Отсутствуют какие-либо известные дефекты		0
7. Необходимый уровень защищенности		
Необходимо соблюдение строгой конфиденциальности, содержатся важные для Банка сведения		5
Необходимо соблюдение мер безопасности, содержатся системы управления финансовыми активами		4
Не нужны никакие дополнительные меры безопасности сверх организации обслуживания на время процесса восстановления		0

Приложение №3
к Плану ОНиВД

Типовой порядок информирования (оповещения) заинтересованных лиц о наступлении и функционировании Банка в случае возникновения нестандартных и чрезвычайных ситуаций

Начальнику Службы безопасности Банка:

– сообщить при необходимости дежурному ОВД, уполномоченным органам МЧС;

– сообщить руководству Банка;

– организовать оповещение сотрудникам и клиентам Банка при помощи громкой связи (при необходимости).

Управляющий делами:

– обеспечить организацию оповещения сотрудников Банка доступными средствами связи;

– обеспечить по решению ГУЧС размещение необходимой информации на сайте Банка.

Управлению правового обеспечения:

– уведомить налоговые органы о возникновении чрезвычайной ситуации в случае невозможности своевременной отправки информации, предусмотренной налоговым кодексом.

Управлению по работе с корпоративными клиентами, Управлению развития банковских услуг, Центру электронных услуг и обслуживания физических лиц, Управлению «Расчетный центр»:

– согласовать порядок отправки платежей с Отделом расчетных систем и банковских телекоммуникаций, Операционным отделом, УИТ и УПС;

– при невозможности продолжать деятельность в штатном режиме, информировать клиентов Банка о сложившейся нестандартной и чрезвычайной ситуации и об изменениях в порядке работы путем оповещения по телефону, системам I-Bank и «Банк-Клиент», а также иными возможными способами: по мобильному телефону, SMS, объявление и др.

Начальнику КФУ:

– согласовать порядок отправки платежей с Отделом расчетных систем и банковских телекоммуникаций, Операционным отделом и УИТ;

– при невозможности продолжать деятельность в штатном режиме, информировать заемщиков Банка о сложившейся нестандартной и чрезвычайной ситуации и об изменениях в порядке работы путем оповещения по телефону, системам I-Bank и «Банк-Клиент», а также иными возможными способами: по мобильному телефону, SMS, объявление и др.

Всем сотрудникам:

– не делать никаких заявлений для прессы и других средств массовой информации без консультаций с Управлением делами.

Заинтересованное лицо	**Ответственное лицо за своевременное информирование**
Клиенты (РКО – юридические, физические лица, ИП) I-BANK СМИ, web-сайт Банка Телефон, электронная почта	Вице-президент (курирующий данное направление) Начальник УИТ Управляющий делами Вице-президент (курирующий данное направление)
Клиенты (физические лица, платежные карты, таможенные карты), ВИП-Клиенты,	Заместитель Президента Банка
Клиенты (кредитный блок)	Вице-президент (курирующий данное направление)
Государственные органы	Вице-президент (курирующий данное направление)

Приложение №4
к Плану ОНиВД

Телефонный справочник

1. Основные контакты.

1.1. Телефоны контролирующих органов.

– Банк России – 8 (495) 771-91-00, 8 (800) 250-40-72

– Главное управление Центрального банка Российской Федерации по Центральному федеральному округу г. Москва – 8 (495) 950-21-90

1.2. Телефоны городских служб экстренной помощи (г. Москва).

Звонки в городские службы экстренной помощи (бесплатно):

101 / (01) - пожарная охрана и спасатели

102 / (02) - милиция

103 / (03) - скорая помощь

104 / (04) - газовая аварийная служба

911 / 112 - один из телефонов экстренной помощи, используемых в стандарте GSM. Вызов доступен даже при блокировке клавиатуры мобильного телефона.

Внимание!

При звонках с некоторых моделей аппаратов, не поддерживающих набор короткого номера, следует набирать номера служб экстренной помощи в полном международном формате:

– международный префикс «+»;

– код страны;

– код города;

– номер телефона.

ПРИ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ, СТИХИЙНЫХ БЕДСТВИЯХ, КАТАСТРОФАХ	
Пожарные и спасатели	01
МГПС (Московская городская поисково-спасательная служба) (круглосуточно)	(495) 917-1502, 917-2595, 917-2583
МЧС России, оперативный дежурный (круглосуточно)	(495) 926-3738, 926-3739
Служба спасения (круглосуточно), все виды оказания помощи	(495) 937-9911
Служба спасения «Гранд-Вымпел», городская спасательная служба при МЧС (круглосуточно)	(495) 995-1068, 164-3332
Центр «Лидер» МЧС России. Проведение спасательных операций особого риска.	(495) 339-7688
Центр управления кризисных ситуаций Москвы, дежурная служба (круглосуточно)	(495) 995-9999, 499-9999, 244-8303
АСБОН (филиал МЧС), экстренное открытие замков дверей квартир, гаражей, машин, сейфов (круглосуточно)	(495) 799-8888
Московское управление милиции на воздушном транспорте	(495) 214-0805, 214-0811
Московское управление милиции на железнодорожном транспорте	(495) 264-6834
Центроспас МЧС РФ, поисково-спасательная служба по г. Москве (круглосуточно)	
- Центральная база	278-9596
- База № 2	426-8900, 426-5980
- База в г. Зеленограде	531-2000, 531-6666
Управление по делам ГО и ЧС административных округов г. Москвы (круглосуточно):	
- Восточный АО	267-4843
- Западный АО	149-2431

- Зеленоградский АО	535-1601
- Северный АО	450-8639
- Северо-Восточный АО	281-5920
- Северо-Западный АО	192-8095
- Центральный АО	912-5807
- Южный АО	319-7718
- Юго-Восточный АО	350-3862, 175-3550
- Юго-Западный АО	121-9200
ПРИ ХИМИЧЕСКОМ, РАДИАЦИОННОМ, ЭКОЛОГИЧЕСКОМ ЗАГРЯЗНЕНИИ	
Демеркуризация помещений и территорий. НПП «Экотром»	110-0001
Управление по борьбе с правонарушениями в области охраны окружающей среды	254-7556
Санэпидемстанция (оперативный дежурный, круглосуточно)	287-3141
Центр «Лидер» МЧС России. Проведение спасательных операций особого риска.	пейджер 926-3522 аб.840
Green Peace (по будням с 10-00 до 18-00 час.)	257-4116
ПРИ ПОЖАРЕ	
Пожарные и спасатели	01
Главное управление государственной противопожарной службы МВД РФ	217-2059
Управление государственной противопожарной службы ГУВД Москвы	244-8233
ПРИ АВАРИЯХ – КОММУНАЛЬНЫЕ СЛУЖБЫ	
Мосгаз	04
Мосгаз. Центральная городская диспетчерская газовой сети	917-4316, 917-4525
Мосгорсвет. Дежурный диспетчер (уличное освещение)	928-8802
ПРИ ПРЕСТУПЛЕНИЯХ И ПРАВОНАРУШЕНИЯХ	
Федеральная служба безопасности РФ (ФСБ России)	921-0762
Министерство по налогам и сборам РФ	913-0009
Управление ГИБДД г. Москвы	923-3390, 923-4909
Министерство внутренних дел РФ	237-8551
- Главное управление по борьбе с организованной преступностью МВД РФ	204-8815
- Главное управление вневедомственной охраны МВД РФ	251-4051
- Главное управление обеспечения охраны общественного порядка МВД РФ	239-6428
- ГУВД Московской области	222-4801
Территориальные подразделения УВД административных округов г. Москвы (дежурные части):	
УВД Центрального АО (Б. Полянка ул., 7/10, стр. 2)	953-2967
УВД Северо-Восточного АО (Вешних вод ул.,10, корп.3)	183-0101
УВД Восточного АО (5-я Парковая ул.,38/13)	965-1401
УВД Юго-Восточного АО (Сормовский пр., д. 13, корп. 2)	919-1962
УВД Южного АО (Каширское шос., 30)	324-8802
УВД Западного АО (2-й Мосфильмовский пер., 8)	147-4220
УВД Северного АО (Адмирала Макарова ул., 23, корп. 1)	452-4945
СКОРАЯ МЕДИЦИНСКАЯ ПОМОЩЬ И ГОСПИТАЛИЗАЦИЯ	03
Научно-практический центр экстренной медицинской помощи (круглосуточно). Экстренный вызов при ДТП, взрывах, чрезвычайных	924-8138, 924-8110

ситуациях	
Институт им. Склифосовского, приемное отделение (круглосуточно)	280-9360, 280-4154, 929-1009
Госпитализация, перевозка рожениц и гинекологических больных (круглосуточно)	684-0026
Скорая и неотложная помощь, госпитализация (платная, круглосуточно) «Медэкспресс»	401-5470
Городской центр экстренной психологической помощи (9-00 – 20-00)	924-6001

Приложение №5
к Плану ОНиВД

План эвакуации

Планы эвакуации располагаются на каждом этаже здания.

Особенности эвакуации сотрудников кассового узла и ведущего специалиста по сейфовым ячейкам:

– устное распоряжение о прекращении работы сейфовых ячеек, кассового узла и перемещении денежных ценностей из приходно-расходных касс в хранилище ценностей при наступлении нестандартной и чрезвычайной ситуации отдает Президент Банка, а в случае его отсутствия – его заместитель, ответственный за сохранность денежных ценностей Банка.

– сотрудники кассового узла Банка под руководством Начальника Отдела налично-денежных операций помещают денежную наличность в мешки для перевозки ценностей, пломбируют мешки и передают их Заведующему кассой Банка. Заведующий кассой и Начальник Отдела налично-денежных операций перемещает полученные от кассиров мешки с ценностями и иные ценности находящиеся в кассе Банка в хранилище ценностей Банка.

– хранилище ценностей Банка закрывается ответственными за сохранность ценностей сотрудниками и, при технической возможности, сдается под охрану техническими средствами охранной сигнализации.

– хранилище ценностей клиентов закрывается ведущим специалистом по сейфовым ячейкам, а в случае его отсутствия Начальником Отдела налично-денежных операций и, при технической возможности, сдается под охрану техническими средствами охранной сигнализации.

– после этого сотрудники кассового узла Банка и ведущий специалист по сейфовым ячейкам эвакуируются.

Приложение №6
к Плану ОНиВД

Перечень проводимого обучения

Тема обучения	Ответственное за обучение структурное подразделение Банка	Обучаемое структурное подразделение Банка	Периодичность проводимого обучения	Комментарии
В области охраны и поддержания непрерывности действия пропускного режима	Служба безопасности	Служба безопасности; Отдел материально-технического обеспечения Управления делами	Не реже одного раза в два года	В соответствии с разработанной программой обучения
В области информационной безопасности	Отдел информационной безопасности Службы безопасности	Все структурные подразделения Банка	На постоянной основе и при выявлении проблем в процессе работы	Во взаимодействии с Управлением информационных технологий, в соответствии с разработанными в Банке Регламентами (Политиками) по информационной безопасности
В области функционирования систем телефонии и средств связи	Управление информационных технологий	Управление информационных технологий; Отдел информационной безопасности Службы безопасности; Отдел материально-технического обеспечения Управления делами	Не реже одного раза в два года	Во взаимодействии с Отделом материально-технического обеспечения Управления делами в соответствии с разработанной программой обучения
В области информационных технологий	Управление информационных технологий	Управление информационных технологий; Отдел информационной безопасности Службы безопасности; Отдел материально-технического обеспечения Управления делами	Не реже одного раза в два года	Во взаимодействии с Отделом информационной безопасности СБ в соответствии с разработанной программой обучения
		Все структурные подразделения Банка (сотрудники/владельцы АРМ)	На постоянной основе и при выявлении проблем в процессе работы	Во взаимодействии с Отделом информационной безопасности СБ в соответствии с проводимыми инструктажами при установке АРМ, программных комплексов.

В области энергоснабжения	Отдел материально-технического обеспечения Управления делами	Все структурные подразделения Банка	Не реже одного раза в два года	Во взаимодействии с арендодателем занимаемых Банком помещений, в соответствии с разработанной программой обучения и утвержденными инструктажами.
В области противопожарной охраны		Все структурные подразделения Банка	Не менее одного раза в год	
При затоплениях		Все структурные подразделения Банка	Не реже одного раза в два года	
В области охраны здоровья	Отдел по работе с персоналом Управления делами при участии Отдела материально-технического обеспечения Управления делами	Все структурные подразделения Банка	Не реже одного раза в два года	Во взаимодействии с: - Управлением правового обеспечения, в соответствии с разработанной программой обучения и утвержденными инструктажами по технике безопасности.
В области кадровой политики	Отдел по работе с персоналом Управления делами	Отдел по работе с персоналом Управления делами: Управление правового обеспечения	Не реже одного раза в два года	Во взаимодействии с Управлением правового обеспечения в соответствии с разработанной программой обучения
В области противорадиационной защиты	Управление «Расчетный центр»	Сотрудники Центральной операционной кассы Управления «Расчетный центр»	Не менее одного раза в год	Во взаимодействии с Отделом материально-технического обеспечения Управления делами, в соответствии с разработанной программой обучения
В области правового обеспечения	Управление правового обеспечения	Управление правового обеспечения; Отдел по работе с персоналом Управления делами	Не реже одного раза в два года	В соответствии с разработанной программой обучения
В области обеспечения и организации мероприятий по гражданской обороне и чрезвычайным ситуациям	Отдел информационной безопасности Службы безопасности	Все структурные подразделения Банка	Ежегодно, в объеме не менее 16 часов	В соответствии с Программой курсового обучения сотрудников в области гражданской обороны и чрезвычайным ситуациям в Банке
		Лица, принимаемые на работу в Банк	При приеме на работу	В соответствии с Программой вводного инструктажа по гражданской обороне и предотвращению чрезвычайных ситуаций в Банке

Приложение №7
к Плану ОНиВД

Личная карточка сотрудника обучения

Ф. И. О.	**Структурное подразделение**	**Должность**	**Дата приема/перевода на работу**

Уровень образования _____

Навыки _____

Опыт и квалификация _____

Дата проведения обучения по Плану ОНиВД	Вид обучения/ проверки	Причина проведения	Обучен/ проверен	Подпись сотрудника	Результат (уд/неуд.)	ФИО обучающего/ проверяющего	Подпись обучающего