ПРОЕКТ

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛОЖЕНИЕ

от __ _____2018 г. № ____-П

О ТРЕБОВАНИЯХ К СИСТЕМЕ УПРАВЛЕНИЯ ОПЕРАЦИОННЫМ РИСКОМ В КРЕДИТНОЙ ОРГАНИЗАЦИИ И БАНКОВСКОЙ ГРУППЕ

На основании статьи 57.1 Федерального закона от 10 июля 2002 года № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2003, № 2, ст. 157; № 52, ст. 5032; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 25, ст. 2426; № 30, ст. 3101; 2006, № 19, ст. 2061; № 25, ст. 2648; 2007, № 1, ст. 9, ст. 10; № 10, ст. 1151; № 18, ст. 2117; 2008, № 42, ст. 4696, ст. 4699; № 44, ст. 4982; № 52, ст. 6229, ст. 6231; 2009, № 1, ст. 25; № 29, ст. 3629; № 48, ст. 5731; 2010, № 45, ст. 5756; 2011, № 7, ст. 907; № 27, ст. 3873; № 43, ст. 5973; № 48, ст. 6728; 2012, № 50, ст. 6954; № 53, ст. 7591, ст. 7607; 2013, № 11, ст. 1076; № 14, ст. 1649; № 19, ст. 2329; № 27, ст. 3438, ст. 3476, ст. 3477; № 30, ст. 4084; № 49, ст. 6336; № 51, ст. 6695, ст. 6699; № 52, ст. 6975; 2014, № 19, ст. 2311, ст. 2317; № 27, ст. 3634; № 30, ст. 4219; № 40, ст. 5318; № 45, ст. 6154; № 52, ст. 7543; 2015, № 1, ст. 4, ст. 37; № 27, ст. 3958, ст. 4001; № 29, ст. 4348, ст. 4357; № 41, ст. 5639; № 48, ст. 6699; 2016, № 1, ст. 23, ст. 46, ст. 50; № 26, ст. 3891; № 27, ст. 4225, ст. 4273, ст. 4295) и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от __ _____ 2018 года № __) Банк России устанавливает требования к системе управления операционным риском в кредитной организации и банковской группе, включая требования к системам управления риском

информационной безопасности и риском информационных систем, а также ведению аналитической базы данных о событиях операционного риска и потерях, понесенных вследствие его реализации.

Глава 1. Общие положения.

1.1. Кредитные организации создают систему управления риском возникновения прямых и непрямых потерь в результате несовершенства или ошибочных внутренних процессов кредитной организации, действий персонала и иных лиц, сбоев и недостатков информационных, технологических и других систем, а также в результате реализации внешних событий (далее – операционный риск), в соответствии с требованиями настоящего Положения.

1.2. Операционный риск присущ всем направлениям деятельности кредитной организации, процессам и системам.

1.3. Риск возникновения у кредитной организации потерь вследствие нарушения кредитной организацией и (или) ее контрагентами условий заключенных договоров, допускаемых кредитной организацией правовых ошибок при осуществлении деятельности, несовершенства правовой системы, нарушения контрагентами нормативных правовых актов, нахождения филиалов кредитной организации, юридических лиц, в отношении которых кредитная организация осуществляет контроль или значительное влияние, а также контрагентов кредитной организации под юрисдикцией различных государств (далее – правовой риск) является видом операционного риска.

1.4. Риск информационной безопасности (далее – риск ИБ) определяется в соответствии с главой 7.1 настоящего Положения, риск информационных систем (далее – риск ИС), определяется в соответствии с пунктом 8.1 настоящего Положения.

1.5. Фактическая реализация операционного риска (далее – событие операционного риска) фиксируется кредитной организацией в аналитической базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации (далее – база событий).

1.6. Система управления операционным риском в кредитной организации должна состоять из следующих элементов:

процедур управления операционным риском (выявление и идентификация операционного риска, сбор и регистрации информации о внутренних событиях операционного риска и потерях в базе событий, количественная и качественная оценка уровня операционного риска, выбор и применение способа реагирования на операционный риск по результатам оценки, мониторинг операционного риска, контроль за эффективностью управления операционным риском);

классификаторов, используемых в системе управления операционным риском, в соответствии с главой 2 настоящего Положения;

контрольных показателей уровня операционного риска кредитной организации, в соответствии с главой 5 настоящего Положения;

системы мер, направленных на снижение уровня операционного риска, установленной кредитной организацией в соответствии с пунктом 4.1.6. настоящего Положения;

подразделения (работников) кредитной организации (банковской группы) по управлению операционным риском, осуществляющего разработку системы управления операционным риском, включая процедуры управления и методы оценки величины операционного риска и необходимого капитала на его покрытие, составление отчетности, а также обеспечивающего реализацию внедрения системы управления операционным риском в целом и поддержку ее функционирования (далее – подразделение, ответственное за управление операционным риском);

специализированных подразделений кредитной организации, структурно независимыми от подразделения, ответственного за управление операционным риском, которые могут управлять отдельными видами операционного риска, определенными в пункте 2.3.5 настоящего Положения (например, риском ИБ или правовым риском), при этом, когда функции управления отдельными видами операционного риска исполняются

служащими специализированных подразделений, координация деятельности таких служащих, связанная с управлением операционным риском, осуществляется руководителем подразделения, ответственного за управление операционным риском);программного комплекса, обеспечивающего функционирование как в целом системы управления операционным риском, так и отдельных ее элементов;

иных элементов системы управления операционным риском, определенных в соответствии с главой 4 настоящего Положения.

1.7. Исполнительный орган кредитной организации отвечает за создание и функционирование системы управления операционным риском в соответствии с требованиями настоящего Положения, включая риск ИБ и риск ИС, как части системы управления рисками кредитной организации.

1.8. Кредитная организация (головная кредитная организация банковской группы) создает и организует систему управления операционным риском, включая риском ИБ и ИС в соответствии с требованиями к системе управления рисками кредитной организации, установленных в пунктах 3.1, 3.2, 3.4 -3.8 Указания Банка России от 15.04.2015 № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы» (далее – Указание Банка России № 3624-У).

Глава 2. Классификации, используемые в системе управления операционным риском.

2.1. Все события операционного риска, включая события риска информационной безопасности, риска информационных систем классифицируются в разрезе: источников (причин) риска, типов событий, направлений деятельности (бизнес-процессов) и видов потерь.

2.2. Кредитная организация (головная кредитная организация банковской группы) разрабатывает классификаторы источников (причин) риска, направлений деятельности (бизнес-процессов), видов операционного риска, типов событий, видов потерь от реализации операционного риска, включая риск ИБ и ИС, в соответствии с требованиями настоящей главы.

2.3. Источники (причины) операционного риска классифицируются на следующие категории.

2.3.1. К первой категории относятся ошибки и недостатки процессов, в том числе ненадежной и (или) неэффективной организации внутренних процедур управления кредитной организации и проведения банковских и других операций (далее – процедуры), а также несоответствия указанных процедур характеру и (или) масштабам деятельности кредитной организации и (или) требованиям действующего законодательства (далее – ошибки и недостатки процессов).

2.3.2. Ко второй категории относятся риски, связанные с действиями персонала кредитной организации (непреднамеренные ошибки, умышленные действия или бездействие) и иных связанных с кредитной организацией лиц, включая собственников, а также лиц, связанных с кредитной организацией в рамках договорных отношений по выполнению работ (оказанию услуг) для кредитной организации (далее – действия персонала).

2.3.3. К третьей категории относятся отказы (нарушения функционирования) применяемых кредитной организацией информационных, технологических и других систем и (или) недостаточность их функциональных возможностей (характеристик) потребностям кредитной организации (далее – сбои систем);

2.3.4. К четвертой категории относятся воздействия внешних причин, в том числе действия сторонних третьих лиц, в том числе действия государственных и регулирующих органов, правоохранительных органов и иных организаций (далее – внешние события).

2.3.5. Для целей организации управления операционным риском, распределения ответственности и ведения базы событий, операционный риск классифицируется по видам риска в зависимости от процессов кредитной организации, например:

риск ИБ;

риск ИС;

риск управления проектами (далее – проектный риск);

риск ошибок и недостатков управленческих процессов (далее – управленческий риск);

правовой риск;

риск нарушения процедур контроля;

риск ошибок процессов разработки, проверки, адаптации, приемки методик и количественных моделей оценки активов и рисков (далее – модельный риск);

риск персонала.

2.4. Для отдельных видов операционного риска могут выделяться дополнительные категории источников (причин) риска.

2.5. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах определяет последующие уровни классификации источников (причин) событий операционного риска, отражающие причины реализации данных источников риска и (или) нарушений, особенности организации бизнес-процессов, организационной структуры, структуры информационных систем и технологий, характер и масштаб деятельности кредитной организации. Классификация может быть многоуровневой.

2.6. У одного и того же события операционного риска могут быть несколько источников. В этом случае в отношении реализовавшегося события риска в базе событий кредитная организация определяет вес значимости вклада конкретного источника риска в реализацию данного события риска.

2.7. Типы событий, для целей управления операционным риском, классифицируются следующим образом (далее – классификация событий первого уровня):

2.7.1. Внутреннее мошенничество, то есть проведение преднамеренных действий с участием хотя бы одного работника кредитной организации, направленных на присвоение (хищение), уничтожение (нанесение ущерба) материальных и нематериальных активов или иного имущества кредитной

организации, ухудшение работы процессов, недостижение целей кредитной организации, в том числе случаи умышленного несоблюдения законодательства, нормативных актов или внутренних распорядительных документов кредитной организации для цели извлечения материальной и нематериальной выгоды.

2.7.2. Внешнее мошенничество, то есть проведение преднамеренных действий, направленных на присвоение (хищение), уничтожение (нанесение ущерба) материальных и нематериальных активов или иного имущества кредитной организации, ухудшение работы бизнес-процессов и систем, недостижение целей кредитной организации, приобретение прав на имущество кредитной организации обманным путем или в нарушение действующего законодательства, совершаемые с участием третьих лиц, клиентов, контрагентов (без участия работников кредитной организации).

2.7.3. Нарушения кадровой политики и безопасности труда, включая нарушения трудового законодательства, требований по охране труда, охране здоровья или в связи с выплатами по искам о нанесении личного ущерба или искам в связи с дискриминацией, а также вследствие прекращения трудовых отношений.

2.7.4. Нарушения прав клиентов и контрагентов, включая нанесение им ущерба (прямо или косвенно), при оказании им банковских услуг и операций (включая нарушения условий договоров и сохранности конфиденциальной информации, ставшей доступной кредитной организации в процессе взаимодействия с клиентами или контрагентами по банковским операциям и сделкам при оказании банковских услуг и нарушений кодексов поведения на рынках, норм и обычаев делового оборота).

2.7.5. Ущерб материальным (физическим) активам кредитной организации, то есть снижение стоимости имущества, потеря свойств материальных активов кредитной организации вследствие стихийных бедствий, техногенных катастроф, беспорядков и военных действий.

2.7.6. Нарушения функционирования и сбои систем, обеспечивающих функционирование основной деятельности кредитной организации.

2.7.7. Нарушения при организации, исполнении и управлении процессами основной деятельности кредитной организации, включая ошибки при обработке операций, недостатки обеспечения функционирования внутренних процессов, недостатки систем управления рисками, внутреннего контроля, учета и отчетности, системы обеспечения информационной безопасности, недостатки в процессах взаимоотношений с торговыми контрагентами и поставщиками.

2.8. Для отдельных видов операционного риска, для целей классификации событий операционного риска в базе событий, могут применяться дополнительные типы событий в разрезе классификации первого уровня, в соответствии с пунктом 2.7 настоящего Положения.

2.9. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах может определить дополнительные уровни классификации типов событий операционного риска, разработанные с учетом особенностей деятельности кредитной организации. Классификация типов событий операционного риска второго уровня представлена в Приложении 1 настоящего Положения.

Кредитная организация (головная кредитная организация банковской группы) вправе расширить классификацию типов событий до третьего уровня и более, с учетом особенностей деятельности кредитной организации.

2.10. По основным направлениям деятельности (бизнес-процессам) кредитной организации события операционного риска классифицируются следующим образом (далее – классификация направлений деятельности (бизнес-процессов) первого уровня):

корпоративное финансирование – оказание услуг корпоративным клиентам, органам государственной власти и местного самоуправления по организации доступа к рынкам капитала, оптимизации структуры активов и повышения качества корпоративного управления, слияния и поглощения,

оказание консультационных услуг финансового посредничества, в том числе при организации синдицированного кредитования;

операции и сделки на финансовом рынке – осуществление операций и сделок с финансовыми инструментами торгового портфеля;

розничное банковское обслуживание – оказание банковских услуг розничным клиентам, кроме брокерских и депозитарных услуг;

коммерческое банковское обслуживание корпоративных клиентов – оказание банковских услуг юридическим лицам за исключением корпоративного финансирования;

операции по осуществлению платежей и расчетов – осуществление платежей и расчетов, в которых кредитная организация выступает как клиент либо контрагент (например, по хозяйственным операциям, собственным платежам, организация расчетов, клиринговая деятельность), за исключением платежей и расчетов, осуществляемых в рамках обслуживания клиентов по бизнес-процессам других направлений деятельности;

агентские услуги и депозитарные услуги – оказание агентских и депозитарных услуг, в том числе услуг по хранению сертификатов ценных бумаг и (или) их учету, обеспечению сохранности активов и документов клиентов;

управление активами – управление активами клиентов по договорам доверительного управления;

розничное брокерское обслуживание – брокерское обслуживание розничных клиентов.

Кредитная организация (головная кредитная организация банковской группы) вправе расширить классификацию направлений деятельности (бизнес-процессов) до второго уровня и более, с учетом особенностей деятельности кредитной организации.

2.11. Потери кредитной организации в результате реализации операционного риска делятся на прямые и непрямые.

2.11.1. Прямые потери, отраженные на счетах расходов и убытков в бухгалтерском учете, в соответствии с Положением Банка России от 22 декабря 2014 года № 446-П «О порядке определения доходов, расходов и прочего совокупного дохода кредитных организаций», классифицируются по следующим видам:

снижение (обесценение) стоимости активов (например, снижение стоимости материальных активов, в результате начисления амортизационных расходов; потеря активов в результате хищения; потеря наличных денежных средств в результате хищения или физического уничтожения; обесценение стоимости кредита, в результате начисления дополнительных резервов в случае увеличения кредитного риска из-за реализации источника (источников) операционного риска; отрицательная переоценка стоимости торгового портфеля и (или) финансового инструмента из-за нарушения правил совершения сделок и операций с инструментами торгового портфеля, и другие);

досрочное списание (выбытие, потеря, уничтожение) материальных и нематериальных, финансовых активов;

денежные выплаты клиентам и контрагентам, а также служащим кредитной организации в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине кредитной организации;

потери от невозврата ошибочных платежей;

судебные издержки и выплаты по решению суда, в том числе расходы на адвокатов и судебных представителей, по делам, связанным с реализацией событий операционного риска;

штрафы и санкции, наложенных надзорными или административными органами;

расходы на устранение последствий реализации событий операционного риска, направленные на восстановление хозяйственной деятельности или на снижение потерь от событий операционного риска;

прочие расходы, связанные с реализацией событий операционного риска или устранением последствий событий операционного риска.

2.11.2. Непрямые потери (не отраженные в бухгалтерском учете, но косвенно влияющие на финансовый результат и капитал кредитной организации) классифицируются на потери, определяемые расчетным методом в денежном выражении (далее – косвенные потери) и потери, определяемые экспертным путем, не выраженные в денежном выражении (далее – качественные потери).

2.11.2.1. Косвенные потери включают в себя:

недополученные запланированные доходы (например, от простоя при совершении банковских операций);

не полученные доходы от не проведения сделок и операций по причине реализации событий операционного риска;

расходы на оплату услуг привлеченных по отдельным договорам специалистов (например, оценщиков и консультантов), связанные с устранением последствий реализации событий операционного риска, не отнесенные к прямым потерям;

хищения средств клиентов и иных третьих лиц (с раздельным учетом потерь, которые были компенсированы кредитной организацией в составе прямых потерь, которые были компенсированы сторонними третьими лицами (например, страховыми компаниями) и которые не были компенсированы);

потери кредитной организации, не реализовавшиеся в виде прямых потерь, но которые могли бы возникнуть при реализации не выявленных источников риска и (или) неблагоприятного стечения обстоятельств с определённой доверительной вероятностью, например, нарушение работником кредитной организации лимита, которое при данном стечении обстоятельств не привело к прямым потерям (далее – потенциальные потери);

повышение стоимости заимствований (привлечения кредитных средств) в результате события операционного риска;

снижение рыночной стоимости акций кредитной организации из-за события операционного риска;

прочие затраты, связанные с устранением последствий или снижением потерь от возникновения и реализации операционных рисков.

2.11.2.2. Качественные потери включают в себя:

возникновение источников других типов риска (например, кредитного риска, риска потери деловой репутации, риска ликвидности, регуляторного риска);

приостановку деятельности в результате неблагоприятного события (например, технологического сбоя);

отток клиентов;

ограничения или обязательства выполнения невыгодных для кредитной организации действий, накладываемые со стороны судебных и (или) административных органов;

снижение качества предоставления услуг, выполнения банковских операций (например, нарушение регламентированных сроков выполнения процедур и операций);

утечка, потеря или искажение защищаемой и (или) коммерческой информации;

предписания надзорных, правоохранительных органов;

снижение лимитов на межбанковское кредитование;

иные качественные потери.

В случае отражения в базе событий в отношении зарегистрированного события одного из вида качественных потерь, определяется оценка значимости таких потерь в соответствии с принятой в кредитной организации шкалой качественных оценок (например, по четырехуровневой шкале: «очень высокие», «высокие», «средние», «низкие»).

2.12. Кредитная организация вправе ввести дополнительные виды классификации видов потерь во внутренних документах, включая порядок их определения и актуализации.

Глава 3. Требования к процедурам управления операционным риском.

3.1. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах устанавливает процедуры управления операционным риском в соответствии с требованиями настоящей главы.

3.2. Процедура выявления и идентификации операционного риска, включает:

интервью с работниками кредитной организации (опрос), в том числе с руководством кредитной организации, в рамках которого обсуждаются операционные риски и факторы внешней среды, которые могут оказывать влияние на деятельность кредитной организации;

проведение ежегодной самооценки операционного риска и форм (способов) контроля, направленных на их снижение (качественной экспертной оценки операционных рисков) на основе формализованных анкет, в соответствии с требованиями пункта 3.5.1 настоящего Положения;

анализ базы событий операционного риска, в соответствие с пунктом 3.3. настоящего Положения;

анализ динамики ключевых индикаторов риска в разрезе направлений деятельности и основных бизнес-процессов, в соответствии с пунктом 3.8.2. настоящего Положения;

анализ информации работников кредитной организации, направленной в рамках инициативного информирования работниками кредитной организации службы управления рисками;

анализ актов проверок (предписаний Банка России, иных надзорных органов) и информационные письма со стороны надзорных и правоохранительных органов;

анализ информации внутреннего и внешнего аудита кредитной организации;

иные внешние и внутренние источники информации.

Кредитная организация (головная кредитная организация банковской группы) использует результаты процедуры выявления и идентификации операционного риска для проведения процедуры оценки операционного риска и корректного учета связи идентифицированных операционных рисков с событиями операционного риска в базе событий.

3.3. Процедура сбора и регистрации информации о внутренних событиях операционного риска и потерях включает:

выявление и сбор событий операционного риска, предусматривающий экспертное выявление информации и автоматизированное выявление информации из информационных систем о реализовавшихся или возможных к реализации событиях и ввод в базу событий по алгоритмизированным правилам, установленным кредитной организацией во внутренних документах;

классификацию выявленных событий операционного риска, в соответствии с главой 2 настоящего Положения;

определение потерь от событий операционного риска в соответствии с пунктом 3.3.2 настоящего Положения;

регистрацию событий операционного риска в базе событий операционного риска;

обновление информации о событиях операционного риска в базе событий при выяснении новых обстоятельств их реализации, в соответствии с главой 6 настоящего Положения;

актуализацию источников информации о событиях операционного риска и подразделений (центров компетенций), ответственных за их сбор.

3.3.1 Кредитная организация (головная кредитная организация банковской группы) обеспечивает соблюдение процедуры сбора и регистрации информации о внутренних событиях операционного риска и потерях во всех направлениях деятельности и бизнес-процессах с указанием:

подразделения (центра компетенций) по каждому бизнес-процессу, ответственного за выявление и сбор информации о событиях;

правил предоставления информации центрами компетенций в подразделение, ответственное за управление операционным риском не позднее 1 рабочего дня с момента выявления события операционного риска;

показателей, указанных в первом и пятом абзацах пункта 1.1.1 и первом и восьмом абзацах пункта 2.1.1 Приложения 4 к настоящему Положению в разрезе центров компетенций (ключевых показателей эффективности по выявлению событий операционного риска в бизнес-процессах), несоблюдение которых предусматривает ответственность центров компетенций (их руководителей).

3.3.2. Процедура определения потерь от событий операционного риска включает:

выявление прямых и непрямых потерь (включая установление сроков выявления и правил отражения в бухгалтерском учете кредитной организации), с учетом требований пунктов 6.7 – 6.19 главы 6 настоящего Положения;

методы и порядок определения непрямых потерь от события операционного риска в базе событий;

правила выявления расходов, относящихся к операционному риску из общих расходов кредитной организации (для определения прямых потерь);

правила и методы оценки недополученных доходов, связанных с событиями операционного риска (для определения непрямых потерь);

правила и методы определения потенциальных потерь (для определения непрямых потерь);

отбор и назначение экспертов кредитной организации, ответственных за расчет потерь от событий операционного риска в разрезе направлений деятельности (бизнес-процессов), областей компетенции.

Кредитная организация (головная кредитная организация банковской группы) обеспечивает сбор информации о событиях операционного риска, включая тех, по которым у кредитной организации не было прямых потерь с

учетом требований к ведению базы событий операционного риска в соответствии с главой 6 к настоящему Положению.

3.4. Процедура количественной оценки уровня операционного риска, включает:

агрегированную оценку уровня операционного риска по кредитной организации в целом, а также в разрезе направлений деятельности (бизнес-процессов), в соответствии с пунктом 2.10 настоящего Положения, подразделений, видов операционного риска;

оценку необходимого капитала на покрытие операционного риска в целом по кредитной организации и, при необходимости, в разрезе направлений деятельности и видов операционного риска (например, по риску ИБ) с учетом подходов в соответствии с Приложением 5 к настоящему Положению;

оценку ожидаемых потерь от реализации операционного риска по бизнес-процессам, по которым наблюдается соответствующая статистика событий операционного риска, для расчета надбавки на операционный риск и учета в ценообразовании соответствующих банковских услуг и тарифов.

В случае отсутствия у кредитной организации статистики событий операционного риска достаточной для применения процедуры количественной оценки операционного риска, кредитная организация в обязательном порядке применяет процедуру качественной оценки.

3.5. Процедура качественной оценки уровня операционного риска, проводимая в отношении выявленных операционных рисков, в дополнение к количественной оценке, включает:

самооценку операционного риска и форм (способов) контроля, направленных на снижение его уровня (далее – самооценка операционного риска), в соответствии с пунктом 3.5.1 настоящего Положения;

экспертную профессиональную оценку (профессиональное мнение внутренних и внешних экспертов), с учетом установленными кредитной организацией во внутренних документах правилами и порядком определения

правил привлечения внешних экспертов, в том числе с использованием автоматизированной оценки программными комплексами;

сценарный анализ операционных рисков.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает методы проведения качественной оценки во внутренних документах, в том числе с привлечением средств автоматизации процедуры качественной оценки.

Подразделение, ответственное за управление операционным риском в кредитной организации разрабатывает на ежегодной основе план проведения качественной оценки операционного риска, включающий определение ответственных и участвующих подразделений кредитной организации, в рамках планирования своей деятельности, который утверждается единоличным исполнительным органом кредитной организации.

Осуществление оценки в соответствии с планом проведения качественной оценки операционного риска является обязательным для всех подразделений кредитной организации (банковской группы).

3.5.1. Самооценка операционного риска проводится кредитной организацией на регулярной основе, по установленной во внутренних документах методике (в виде анкетирования, выделенных для данной процедуры работников подразделений кредитной организации по всем направлениям деятельности).

Самооценка операционных рисков проводится в отношении всех видов операционного риска (в том числе риска ИБ и риска информационных систем).

Кредитная организация определяет критерии оценки для целей самооценки, документирует методику ее проведения во внутренних документах.

Критерии самооценки операционных рисков, должны содержать:

критерии оценки уровня существенности операционного риска (по четырехуровневой шкале: «очень высокий», «высокий», «средний»,

«низкий»), включая критерии оценки потерь и вероятности присущего операционного риска;

критерии оценки эффективности форм (способов) контролей (с учетом уровня регламентации и автоматизации мер снижения уровня оцениваемого риска), действующих на момент проведения оценки;

критерии оценки уровня остаточного риска.

3.5.2. Кредитная организация (головная кредитная организация банковской группы) разрабатывает требования к проведению экспертной профессиональной оценки уровня операционного риска (профессионального мнения внутренних и внешних экспертов) с указанием сроков, правил и порядка ее проведения.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает методы проведения внутренней экспертной профессиональной оценки во внутренних документах на основе требований к ее проведению.

3.5.3. Кредитная организация (головная кредитная организация банковской группы) разрабатывает во внутренних документах методику сценарного анализа операционных рисков и порядок его проведения.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает критерии проведения сценарного анализа в отношении иных источников операционного риска, а также выявленных операционных рисков, которые не реализовались в кредитной организации, но у которых есть вероятность реализации с высоким уровнем потерь (последствий с негативным влиянием на деятельность кредитной организации).

3.6. Процедура выбора и применения способа реагирования на операционный риск по результатам проведенной оценки, включает:

уклонение от риска (отказ кредитной организации от оказания соответствующего вида услуг и банковских операций в связи с высоким уровнем операционного риска в них);

передача риска (страхование, передача риска другой стороне (контрагенту, клиенту);

принятие риска (готовность кредитной организации принять возможные потери в рамках установленного лимита потерь, с соответствующей процедурой контроля соблюдения лимита);

меры, направленные на снижение уровня операционного риска (разработка кредитной организацией форм (способов) контроля и мер, направленных на снижение уровня операционного риска), включающие:

реинжиниринг бизнес-процессов;

установление дополнительных форм (способов) контролей;

обучение персонала, в том числе участников бизнес-процессов;

применение автоматизированных решений;

иные меры, направленные на снижение уровня операционного риска. Перечень возможных мер, направленных на снижение уровня операционного риска представлен в Приложении 3 к настоящему Положению.

3.7. Кредитная организация (головная кредитная организация банковской группы) определяет методы выбора способа реагирования, в том числе и методы оценки стоимости выбранного способа реагирования.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает меры, направленные на снижение уровня операционного риска с учетом оценки эффективности и стоимости уровня остаточного риска (по результатам реализации мер, направленных на снижение уровня операционного риска).

3.8. Процедура мониторинга операционного риска, включает:

ключевые индикаторы риска, то есть количественные показатели, направленные на измерение и контроль уровня операционного риска в определенный момент времени (далее – КИР);

анализ статистики событий операционного риска;

контроль выполнения мер, направленных на снижение уровня операционного риска и планов мероприятий, направленных на

предотвращение возникновения операционного риска, минимизацию вероятности возникновения и (или) величины потерь;

контроль соблюдения условий выбранных способов реагирования на риски;

мониторинг потоков информации, поступающей от центров компетенций, органов управления кредитной организации, иных источников информации.

3.8.1. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах определяет правила и методы применения процедуры мониторинга операционного риска в зависимости от уровня рисков и способы документирования результатов мониторинга операционного риска.

3.8.2. Кредитная организация во внутренних документах устанавливает требования к КИР и к их документированию, включающие:

количественное измерение КИР;

способы расчета КИР, в том числе с использованием средств автоматизации;

регулярность и своевременность расчета КИР с указанием сроков (периода) расчета КИР (например, в постоянном режиме, раз в неделю, по состоянию на момент закрытия операционного дня);

возможность валидации значений и данных КИР для проверки корректности расчета;

состава информации, необходимой для расчета КИР и их источников, включая способ получения информации;

пороговых значений КИР;

операционного риска (нескольких операционных рисков), которых отслеживает КИР;

ответственного подразделения кредитной организации, отвечающего за предоставление данных для расчета КИР и (или) расчет КИР;

порядка реагирования на превышение пороговых значений КИР.

3.8.3. Кредитная организация (головная кредитная организация банковской группы) устанавливает порядок составления и представления регулярной отчетности о результатах процедуры мониторинга операционного риска и их рассмотрение исполнительным органом кредитной организации (иным коллегиальным органом, например, комитетом по управлению операционным риском). В случае совпадения сроков представления результатов процедуры мониторинга операционного риска со сроком представления внутренней отчетности по операционному риску, допускается направление результатов процедуры мониторинга операционного риска в составе материалов внутренней отчетности по операционному риску в соответствии с пунктами 3.10 настоящей главы и пунктом 4.2 настоящего Положения.

3.9. Кредитная организация (головная кредитная организация банковской группы) предусматривает во внутренних документах, регламентирующих процедуры управления операционным риском, роли и ответственность подразделений кредитной организации, в соответствии с которыми ответственность за выявление операционного риска, сбор информации о событиях операционного риска и потерях, участие в качественной оценке операционного риска закрепляется за всеми структурными подразделениями-участниками бизнес-процессов и подразделениями обеспечивающих процессов кредитной организации.

3.10. Кредитная организация (головная кредитная организация банковской группы) определяет порядок документирования результатов выполнения процедур управления операционным риском и направления их на рассмотрение (не реже двух раз в год) исполнительному органу кредитной организации в составе внутренней отчетности по операционным рискам, в соответствии с пунктом 4.2. настоящего Положения.

3.11. Уполномоченное подразделение, определенное в соответствии с пунктом 4.1.4 настоящего Положения, ежегодно осуществляет оценку качества соблюдения процедур управления операционным риском кредитной

организации. Отчет о результатах оценки качества соблюдения процедур управления операционным риском (в том числе на предмет их полноты и корректности) предоставляется на рассмотрение исполнительному органу кредитной организации.

Глава 4. Требования к отдельным элементам системы управления операционным риском.

4.1. Система управления операционным риском в кредитной организации, за исключением элементов, предусмотренных в абзацах 2-7 пункта 1.6 настоящего Положения, включает следующие отдельные элементы.

4.1.1. Перечень основных бизнес-процессов кредитной организации в разрезе направлений деятельности с указанием функций подразделений – участников процесса, владельца процесса (то есть подразделения, ответственного за разработку методологии процесса и его поддержку), информационных систем, обеспечивающих бизнес-процесс, класса критичности (по трем уровням) информационных систем, а также внешних факторов, которые могут повлиять на процесс и взаимосвязи влияния между другими бизнес-процессами.

4.1.2. Политику (положение) по управлению операционным риском и внутренние документы, описывающие процедуры управления операционным риском, включая риски ИБ и ИС, а также процедуры оценки качества функционирования системы управления операционным риском.

4.1.3. Внутренние документы по структуре и организации в кредитной организации (банковской группе) управления операционным риском, в том числе описание полномочий и функций руководителей подразделений, ответственных за управление операционным риском, риском ИБ и риском ИС и подразделений-владельцев рисков.

4.1.4. Порядок оценки кредитной организацией и (или) внешними экспертами качества функционирования системы управления операционным риском, в том числе выполнения принятых в кредитной организации процедур по управлению операционным риском.

Кредитная организация (головная кредитная организация банковской группы) определяет подразделение, структурно независимое от службы управления рисками, уполномоченное проводить оценку качества функционирования системы управления операционным риском (включая риск ИБ и ИС), в том числе оценку качества выполнения принятых в кредитной организации процедур по управлению операционным риском, риском ИБ и ИС (далее – уполномоченное подразделение), а также вправе привлекать для оценки качества функционирования системы управления операционным риском внешних экспертов.

4.1.5. Систему мер, направленных на снижение уровня операционного риска, включающую меры, направленные на предотвращение (снижение вероятности) событий операционного риска и меры, направленные на ограничение размера потерь от событий операционного риска.

Меры, направленные на предотвращение (снижение вероятности) событий операционного риска, включают:

разработку процедур совершения операций (сделок), порядка разделения полномочий и подотчетности по проводимым операциям (сделкам), позволяющих исключить (ограничить) возможность реализации события операционного риска;

контроль за соблюдением установленных процедур;

разграничение конфликта интересов;

повышение эффективности процедур контроля в кредитной организации, документирования их результатов.

Меры, направленные на ограничение размера потерь от событий операционного риска, включают:

ведение лимитов полномочий и лимитов операционного риска, контроля за соблюдением полномочий;

развитие систем автоматизации бизнес-процессов и защиты информации;

разработка планов по обеспечению непрерывности ключевых бизнес-процессов и информационных систем, включая цифровую инфраструктуру, а также безопасности и целостности информационных систем и информации, в том числе в соответствии с требованиями главы 8 настоящего Положения;

разработку планов восстановления деятельности кредитной организации, в случае реализации операционного риска и системы быстрого реагирования на события операционного риска с критичным уровнем потерь;

способ и порядок возмещения потерь от реализации событий операционного риска, с использованием страхования, включая, имущественное страхование (страхование зданий, иного имущества, включая валютные ценности и ценные бумаги, от утраты (гибели), недостачи или повреждения, в том числе в результате действий третьих лиц, работников кредитной организации, а также страхование гражданской ответственности руководителей кредитной организации, связанное с риском возникновения потерь вследствие реализации рисков) и личное страхование (страхование работников от несчастных случаев и причинения вреда здоровью);

правовое сопровождение судебных исков со стороны третьих лиц;

юридическая проработка процессов, договоров и документации кредитной организации.

Указанные мероприятия должны быть доведены головной кредитной организацией банковской группы до дочерних кредитных организаций и иных участников банковской группы.

4.1.6. Кредитная организация (головная кредитная организация банковской группы) разрабатывает способы мотивации персонала к участию в управлении операционным риском, в части:

инициативного информирования о возможных операционных рисках и выявленных персоналом событий операционного риска;

участию в процедурах управления операционным риском, в том числе в процедуре качественной оценки операционного риска;

направления предложений по мерам минимизации операционного риска;

иных форм участия персонала кредитной организации.

4.2. Подразделение, ответственное за управление операционным риском регулярно (не реже 1 раза в квартал) формирует и направляет на рассмотрение исполнительному органу кредитной организации внутреннюю отчетность по операционному риску.

4.2.1 Исполнительный орган управления в установленные сроки рассматривает внутреннюю отчетность по операционным рискам кредитной организации и дает поручения по разработке мер, направленных на снижение уровня операционного риска, с указанием ответственных подразделений за реализацию мер и сроков выполнения.

Внутренняя отчетность по операционным рискам должна храниться в кредитной организации не менее 10 лет со дня рассмотрения исполнительным органом управления и предоставляться Банку России для целей надзорной оценки системы управления операционным риском в кредитной организации в соответствии с пунктом 9.3 настоящего Положения.

4.2.2 Внутренняя отчетность кредитной организации (головной кредитной организации банковской группы) по операционным рискам включает информацию о событиях реализации операционного риска в разрезе отдельных видов операционного риска, в соответствии с пунктом 2.3.5 настоящего Положения и с учетом дополнительной классификации, предусмотренной пунктом 2.7. настоящего Положения, а также о результатах процедур управления операционным риском, включая риском ИБ и ИС, информацию о результатах количественной и качественной оценках операционного риска, выбранных способах реагирования, результатах мониторинга операционного риска, результатах выполнения мер, направленных на снижение уровня операционного риска и о значениях контрольных показателей уровня операционного риска.

4.2.3. Информация о событиях реализации операционного риска включается в отчетность в разрезе направлений деятельности и основных бизнес-процессов, типов событий и источников риска, в том числе отдельно по видам риска, содержащая в том числе следующие показатели:

общее количество событий – количество всех событий, которые были зафиксированы у кредитной организации с начала года до отчетной даты и в отчетном периоде;

количество событий, принесших кредитной организации потери, которые отразились на балансовых счетах кредитной организации с начала года до отчетной даты и в отчетном периоде;

сумма прямых потерь от реализации событий операционного риска в кредитной организации (участников банковской группы), которые отразились на балансовых счетах кредитной организации (головной кредитной организации банковской группы) с начала года до отчетной даты и в отчетном периоде, в разрезе видов потерь в соответствии с главой 2 настоящего Положения;

сумма прямых потерь от реализации событий операционного риска от участников банковской группы или иных связанных с кредитной организацией лиц, которые отразились на балансовых счетах кредитной организации с начала года до отчетной даты и в отчетном периоде;

сумма прямых потерь, в части затрат на восстановление деятельности в разрезе направлений деятельности (бизнес-процессов) и ключевых бизнес-процессов, типов событий;

максимальная величина прямых потерь от одного события из тех, которые были зафиксированы у кредитной организации с начала года до отчетной даты и в отчетном периоде в разрезе направлений деятельности и ключевых бизнес-процессов;

максимальная сумма прямых потерь от пяти событий из тех, которые были зафиксированы у кредитной организации с начала года до отчетной даты

и в отчетном периоде в разрезе направлений деятельности (бизнес-процессов) и ключевых бизнес-процессов;

сумма косвенных потерь с начала года до отчетной даты и в отчетном периоде в разрезе направлений деятельности (бизнес-процессов) и ключевых бизнес-процессов, типов событий;

сумма возмещений по потерям за счет не связанных с кредитной организацией лиц, которые отразились на балансовых счетах кредитной организации с начала года до отчетной даты и в отчетном периоде в разрезе направлений деятельности и ключевых бизнес-процессов, типов событий;

сумма возмещений по потерям за счет связанных с кредитной организацией лиц с начала года до отчетной даты и в отчетном периоде в разрезе направлений деятельности и ключевых бизнес-процессов, типов событий;

сумма чистых потерь, то есть сумма потерь с учетом суммы возмещения, которые были отражены на балансовых счетах кредитной организации с начала года до отчетной даты и в отчетном периоде;

средняя величина потерь от одного события операционного риска в целом, в разрезе направлений деятельности (бизнес-процессов), ключевых бизнес-процессов, типов событий;

среднеквадратичное отклонение (сигма) величины потерь от событий реализации операционного риска в разрезе направлений деятельности (бизнес-процессов), ключевых бизнес-процессов, типов событий.

4.3. Кредитная организация (головная кредитная организация банковской группы) устанавливает требования к информационной системе, обеспечивающей управление операционным риском, включающую автоматизацию ведения базы событий операционного риска и процедур управления операционным риском.

Кредитная организация (головная кредитная организация банковской группы) в зависимости от характера и масштаба осуществляемых операций и действующих бизнес-процессов, осуществляет интеграцию информационной

системы, обеспечивающей управление операционным риском, с другими информационными системами кредитной организации, позволяющими получать первичную информацию о сбоях, ошибках, отклонениях в процессах кредитной организации и реализации рисков ИБ и информационных систем.

4.4. Уполномоченное подразделение ежегодно осуществляет оценку качества функционирования системы управления операционным риском (включая риск ИБ и ИС), включающей оценку:

полноты и точности информации, отраженной в базе событий, а также корректности ведения базы событий операционного риска и риска ИБ;

правильности определения видов и величины потерь от событий операционного риска;

соблюдения установленных в политике управления операционным риском, во внутренних документах требований, порядков и процедур управления операционным риском;

корректности проведенных оценок операционного риска в соответствии с пунктами 3.4-3.5 настоящего Положения;

системы мер, разрабатываемых в соответствии с пунктом 4.1.5 настоящего Положения;

эффективности мер, направленных на снижение уровня операционного риска.

Уполномоченное подразделение устанавливает порядок информирования, исполнительных органов кредитной организации (головной кредитной организации банковской группы), должностного лица, отвечающего за управление рисками, должностного лица, отвечающего за обеспечение информационной безопасности, подразделения, ответственного за управление операционным риском, о выявленных недостатках в системе управления операционным риском в кредитной организации (банковской группе, дочерней организации) и действиях, предпринятых для их устранения.

4.5. Кредитная организация (головная кредитная организация банковской группы) проводит регулярный (не реже 1 раза в год) пересмотр

требований политики управления операционным риском в зависимости от характера и масштаба осуществляемых операций, действующих бизнес-процессов, изменяющихся факторов внешней среды, результатов процедур управления операционным риском (включая риском ИБ и ИС), результатов оценки качества функционирования системы управления операционным риском уполномоченным подразделением.

Глава 5. Требования к системе контрольных показателей уровня операционного риска.

5.1. В целях контроля за уровнем операционного риска кредитная организация (головная кредитная организация банковской группы) определяет на плановый годовой период в соответствии с Приложением 4 к настоящему Положению количественные и качественные контрольные показатели уровня операционного риска, включая риск ИБ, а также устанавливает целевые уровни этих показателей: сигнальный (приемлемый) уровень и контрольный (лимитный).

5.2. Исполнительный орган кредитной организации:

утверждает сигнальные (приемлемые) и контрольные (лимитные) значения количественных контрольных показателей уровня операционного риска и риска ИБ на плановый годовой период (далее – сигнальный показатель и контрольный показатель соответственно), которые ежегодно пересматриваются и актуализируются в рамках регулярной процедуры пересмотра политики управления операционным риском по результатам оценки качества функционирования системы управления операционным риском, в соответствии с пунктом 4.5. настоящего Положения.

обеспечивает контроль за фактическими значениями сигнальных и контрольных показателей;

обеспечивает реагирование кредитной организации в случае превышения контрольных показателей уровня операционного риска.

5.3. Подразделение, ответственное за управление операционным риском регулярно проводит расчет сигнальных и контрольных показателей и

предоставляет их на рассмотрение исполнительному органу кредитной организации на основе статистических данных о событиях операционного риска и риска ИБ за период не менее 10 лет.

В случае, когда период ведения базы событий меньше 10 лет, расчет производится на основе фактически имеющего периода наблюдений с последующим добавлением данных за новые годы, по мере их накопления, вплоть до полных 10 лет. При этом недостаточность данных учитывается в сценариях, применяемых в сценарном моделировании.

Подразделение, отвечающее за управление операционным риском, оформляет расчет и обоснование значений сигнальных и контрольных показателей уровня операционного риска, включая показатели риска ИБ в виде мотивированного суждения и включает в состав материалов, выносимых данным подразделением на рассмотрение исполнительным органом кредитной организации при утверждении (пересмотре) политики управления операционным риском.

5.4. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок действий, роли и ответственность органов управления и структурных подразделений кредитной организации, должностных лиц, в случае нарушения установленных значений контрольных и сигнальных показателей, а также определяет процедуры разработки, утверждения и контроля исполнения системы мер, направленных на снижение уровня операционного риска, мер по устранению источников (причин) операционных рисков, включая рисков ИБ, по причине которых произошли нарушения контрольных и сигнальных показателей.

Глава 6. Требования к ведению базы событий операционного риска.

6.1. Кредитная организация (головная кредитная организация банковской группы) ведет на постоянной основе базу событий, соответствующую требованиям настоящей главы.

6.2. Кредитная организация (головная кредитная организация банковской группы) вправе определить ведется ли база событий консолидировано по банковской группе или раздельно по участникам группы. В случае раздельного ведения базы событий участники группы на ежемесячной основе представляют данные о потерях от реализации событий операционного риска в головную организацию банковской группы в целях расчета капитала группы, необходимого на покрытие операционного риска.

Порядок отчетности участников группы устанавливает головная организация банковской группы в своих внутренних документах, предусмотрев единую классификацию и правила ведения базы событий, а также способы и порядок обмена информацией между участниками группы.

6.3. Порядок ведения базы событий, включая требования к форме и содержанию вводимой информации, должен быть установлен в документах кредитной организации (банковской группы).

6.4. Данные о событиях операционного риска и потерях должны охватывать всю деятельность кредитной организации, все подразделения, организационные, информационные и технологические системы и регионы присутствия кредитной организации (дочерних организаций).

Кредитная организация обеспечивает наличие в базе событий подробной информации о причинах и обстоятельствах, произошедших событиях операционного риска.

6.5. Порог регистрации в базе событий, выявленных событий операционного риска, не устанавливается.

6.6. База событий кредитной организации должна содержать как минимум следующую информацию:

уникальный порядковый идентификационный номер события;

идентификатор группы однородных событий (если событие не единичное);

информацию о дате и времени, когда событие произошло или впервые началось («дата возникновения (дата реализации)»);

информацию о дате и времени, когда кредитной организации стало известно о событии операционного риска («дата обнаружения (дата выявления)»;

информацию о дате и времени окончания события (дата окончания события»);

статус события (установлены ли все обстоятельства события, определены ли потери или в процессе выяснения (определения);

подразделение, в котором произошло событие;

подразделение, выявившее событие;

описание события (детализированное описание события, которое включает ответы на вопросы: в чем заключается событие, каким образом оно было обнаружено, что явилось его причиной (причинами), если потери не возникли, то, что послужило этому причиной);

категории источника (причины) риска, в соответствии с пунктом 2.3 настоящего Положения;

основной источник, который повлиял на реализацию события, согласно экспертному мнению работника кредитной организации;

тип события, в соответствии с пунктом 2.7. настоящего Положения;

вид операционного риска (риск ИБ, правовой риск и другие, в соответствии с пунктом 2.3.5. настоящего Положения);

связь с иными видами риска (кредитный, рыночный, ликвидности, стратегический, репутационный и другие);

иной риск является источником (следствием) события операционного риска;

идентификатор связанного события операционного риска;

дополнительная классификация типа событий в зависимости от вида риска;

направление деятельности, в соответствии 2.10. настоящего Положения;

бизнес-процесс, согласно принятым внутренним документам кредитной организации

шаг бизнес-процесса, согласно принятым внутренним документам кредитной организации

информационная система (если задействована на выполнении шага бизнес-процесса).

Группа полей базы событий, содержащая информацию о потерях от реализации события операционного риска, по каждому виду потерь и возмещений, включающая:

вид потерь, в соответствии с пунктом 2.11. настоящего Положения;

признак связи потери с иным риском;

сумма валовых потерь, в соответствии с пунктом 6.7. настоящего Положения, в рублях;

дата учета потерь, то есть дата отражения операционных потерь на счетах бухгалтерского учета (для событий правового риска дата учета является дата создания резерва-оценочного обязательства некредитного характера)

информация о проводке в бухгалтерском учете суммы потерь;

экспертная оценка качественных потерь, в соответствии с пунктом 2.11.2.2. настоящего Положения.

Группа полей базы событий, содержащая информацию о полученном возмещении понесенных потерь, в соответствии с пунктом 6.17. настоящего Положения:

мероприятия, осуществленные кредитной организацией в целях получения возмещения по понесенным потерям;

вид возмещений (например, в судебном порядке, внесудебном, получение страховой выплаты, компенсации от иных источников);

признак связи возмещения с компенсацией потерь от кредитного риска;

сумма возмещений в рублях;

дата учета возмещения (дата отражения возмещения на счетах бухгалтерского учета);

информация о проводке в бухгалтерском учете суммы возмещения;

источники получения возмещения (от страховой компании, входящую в банковскую группу, от страховой компании, не входящую в банковскую группу, от аффилированных с банковской группой лиц, от контрагента, от иных лиц, от персонала кредитной организации).

Сумма чистых (фактических) потерь (после учета возмещения).

Если сумма потерь и возмещений отражается в иной валюте, отличной от рубля, то пересчет в рубли отражается в базе событий по курсу на дату учета.

Кредитная организация может добавлять иные поля в базу событий.

6.7. Валовые потери определяются как сумма фактических потерь от реализации операционного риска до учета возмещения.

6.7.1. В расчет величины валовых потерь включаются:

прямые потери от события операционного риска, в соответствии с пунктом 2.11.1 настоящего Положения, включая обесценение, списание активов, отраженные на счетах бухгалтерского учета кредитной организации;

расходы на восстановление деятельности после реализации событий операционного риска, в соответствии с пунктом 2.11.1 настоящего Положения;

расходы, выплачиваемые третьим лицам, в связи с реализацией события операционного риска (например, судебные издержки, выплаты, связанные с судебным решением и сборы, выплачиваемые консультантам, адвокатам или поставщикам);

расходы на создание резервов по счетам бухгалтерского учета для покрытия потерь от реализации события операционного риска с учетом видов резервов;

потери, отраженные на иных счетах бухгалтерского учета, не связанные с балансовыми счетами расходов;

корректировку стоимости потерь, связанных с перерасчетом стоимости потерь от реализации события операционного риска прошлого периода в случае, когда отражение в бухгалтерском учете потерь длится более одного календарного года (далее – «распределенные во времени потери»).

6.7.2 Кредитные организации во внутренних документах определяют порядок идентификации потерь и возмещений, с указанием дат учета, сумм и реквизитов проводок в разрезе всех событий, повлекших потери.

6.7.3. В валовые потери не включаются и в базе событий отдельно учитываются:

расходы кредитной организации по договорам с поставщиками на поддержание систем жизнеобеспечения, технических систем, регулярного обслуживания систем;

расходы кредитной организации (внутренние и внешние), направленные на улучшение деятельности после потерь от реализации операционного риска (модернизация, совершенствование, инициативы по предотвращению риска, оценке рисков и расширение функционала по управлению рисками);

выплата страховых премий.

6.8. Кредитная организация (головная кредитная организация банковской группы) должна предусмотреть в базе событий поля связи события операционного риска с иными рисками (кредитный, рыночный, ликвидности, стратегический, репутационный и иные) или другого события операционного риска, в случае если такая связь определена, и обеспечить их учет во внутренних информационных системах и базе событий (базах событий) с учетом их взаимосвязи с предшествующими или последующими событиями операционного риска.

6.9. Кредитная организация (головная кредитная организация банковской группы) учитывает потери в результате реализации событий операционного риска, связанных с иными финансовыми и нефинансовыми

рисками (например, кредитный, рыночный, ликвидности, стратегический, репутационный и иные) в базе событий операционного риска с пометкой о связи с иным риском (например, для возможности выделения потерь от кредитного риска). К указанным событиям операционного риска применяются все иные процедуры управления операционными рисками, предусмотренные главой 3 настоящего Положения, в сочетании с процедурами управления иными рисками, используемыми кредитной организацией.

6.10. По одному и тому же событию операционного риска могут выявляться и учитываться в базе событий несколько видов и величин потерь. Каждая потеря отражается в базе событий отдельной записью с указанием номера проводки, даты учета и с пометкой о связи с иным риском (при необходимости).

6.11. Кредитная организация (головная кредитная организация банковской группы) вправе вести учет потерь от событий всех видов операционного риска (например, риск ИБ, правовой риск и других) и иных нефинансовых рисков как в составе базы событий, так и раздельно. При этом кредитная организация устанавливает единый подход к идентификации, оценке и классификации, в соответствии с главой 2 настоящего Положения, исключающий дублирование и пропуски информации, в целях определения количественных показателей, в соответствии с Приложением 4 к настоящему Положению. В случае, когда события операционного риска одновременно могут быть отнесены к разным нефинансовым рискам (например, когда реализация одного вида риска является источником или результатом другого вида риска) должен быть предусмотрен идентификатор связи этих событий.

6.12. В случае, если кредитная организация ведет отдельную базу событий регуляторного риска, то прямые потери от его реализации включаются в валовые потери от событий операционного риска, с учетом исключения пропусков и дублирования потерь, связанных с раздельным ведением баз событий.

6.13. В случае, когда у события операционного риска потери распределены по разным учетным периодам (годам), то данные потери в базе событий должны быть отнесены к соответствующим годам отражения на счетах бухгалтерского учета.

6.14. Кредитная организация (головная кредитная организация банковской группы) разрабатывает специальные критерии для определения данных о потерях, вызванных единичными событиями реализации операционного риска и от подобных или связанных событий в течение некоторого времени («группа потерь»).

6.15. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах критерии группировки событий (например, события операционного риска могут быть связаны в одну группу, если у них одинаковый источник риска, бизнес-процесс, а период времени возникновения от 1 часа до 24 часов). Группировка событий должна быть предметом оценки, проводимой уполномоченным подразделением.

6.16. Кредитная организация (головная кредитная организация банковской группы), применяющая передовые международные подходы для оценки необходимого капитала на покрытие операционного риска, в соответствии с пунктом 4.9.2 Указания Банка России №3624-У (далее - продвинутый подход), должна накапливать информацию о внешних событиях реализации операционных рисков в других кредитных и финансовых организациях, по составу и масштабу операций сопоставимых с кредитной организацией, включающую данные о суммах потерь, об объеме операций кредитных организаций в регионе, в котором были понесены потери, о причинах и обстоятельствах их возникновения. Эти данные кредитная организация может использовать для сценарного анализа операционного риска, в том числе стресс-тестирования и определения необходимого капитала на покрытие потерь от операционного риска.

6.17. Возмещение является независимым событием, связанным с первоначальным событием потерь, отдельным во времени, в котором средства или приток экономических выгод поступают от третьего лица (например, платежи, полученные от страховщиков, выплаты, полученные от совершивших мошенничество лиц и возврат неверно направленных переводов).

Подразделение, ответственное за управление операционным риском осуществляет контроль за своевременностью учета возмещению по потерям от событий операционного риска.

6.18. В базе событий кредитные организации должны использовать потери за вычетом возмещения (за исключением выплат страховых компаний, входящих в банковскую группу, компенсаций от иных физических и юридических лиц или организаций, способных оказать влияние на деятельность кредитной организации). Возмещение может быть использовано для уменьшения потерь только после того, как платеж получен кредитной организацией и отражен на счетах бухгалтерского учета. Дебиторская задолженность не может являться возмещением.

Учет возмещений должен включаться в программу оценки качества функционирования системы управления операционным риском кредитной организации, проводимой уполномоченным подразделением.

6.19. Чистые (фактические) потери определяется как потери после вычета суммы возмещения.

6.20. Информация о внутренних событиях операционного риска подлежит валидации до начала использования данных о внутренних событиях операционного риска и потерях в оценке потребности в капитале на покрытие операционного риска и регулярной независимой оценке, проводимой уполномоченным подразделением и (или) внешним экспертом.

6.21. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах устанавливает и

предусматривает ответственность за несоблюдение требований внутренних документов по ведению базы событий, включающая определение:

лиц, ответственных за ведение базы событий;

лиц, предоставляющих информацию для базы событий;

лиц, отвечающих за проверку полноты информации в базе событий и сверку счетов бухгалтерского учета с информацией, отраженной в базе событий;

Глава 7. Требования к управлению риском информационной безопасности.

7.1 Кредитная организация (головная кредитная организация банковской группы), в соответствии с ГОСТ 57580.1-2017 «Защита информации финансовых организаций», Указом Президента Российской Федерации от 05 декабря 2016 года «Об утверждении Доктрины информационной безопасности Российской Федерации», определяет порядок управления риском недостатков процессов обеспечения информационной безопасности, а также несоответствия указанных процессов характеру и (или) масштабам деятельности кредитной организации, требованиям нормативных актов Банка России, положениям национальных стандартов Российской Федерации и иных требований о защите данных, разработанных Банком России в рамках законодательства Российской Федерации о техническом регулировании и стандартизации (далее – риск информационной безопасности).

7.2. Риск ИБ включает в себя:

риск преднамеренного воздействия персонала кредитной организации, третьих лиц и(или) сторонних информационных систем, направленного на несанкционированное получение (хищение), изменение, удаление данных и иной цифровой информации и (или) структуры данных, параметров и характеристик систем (в том числе программного кода) и режима доступа, посредством цифровой инфраструктуры и технологий связи (далее – киберриск);

иные виды рисков ИБ, связанных с обработкой (хранением, уничтожением) информации без использования средств цифровой инфраструктуры.

7.3. В соответствии с пунктом 2.4. настоящего Положения для риска ИБ могут определяться дополнительные источники (причины) реализации риска:

угроза (как специфические условия и факторы, присущие процессам обеспечения защиты информации, создающие потенциальную или реальную опасность нарушения защиты информации и данных);

уязвимость (как недостатки информационной системы или ее компонент, обусловливающее возможность реализации угроз защиты данных и обрабатываемой цифровой информации).

7.4. Фактическая реализация риска ИБ, в том числе киберриска, обусловленная источниками (угрозами) риска ИБ, вследствие которых возникли прямые и непрямые потери кредитной организации (далее – событие (инцидент) риска ИБ) фиксируется в базе событий операционного риска, с присвоением отдельного признака.

Негативное влияние риска ИБ проявляется в виде потерь, перечисленных в пункте 3. Приложения 2 к настоящему Положению.

7.5. Кредитная организация (головная кредитная организация банковской группы) вправе определить ведение базы событий риска ИБ как в общей базе событий операционного риска, так и в отдельной базе. В случае если кредитная организация ведет отдельную базу событий риска ИБ, структурному подразделению, ответственному за обеспечение информационной безопасности (например, если данное подразделение не входит в службу управления рисками) необходимо соблюдать требования к определению и классификации событий риска ИБ, в соответствии с пунктами 2.3 - 2.12 главы 2 и требованиями к ведению базы событий в соответствии с пунктами 6.6 - 6.22 главы 6 настоящего Положения.

7.6. Подразделение кредитной организации, отвечающее за ведение базы событий риска ИБ, классифицирует события рисков ИБ по всем

элементам в соответствии с главой 2 настоящего Положения, и использует элементы дополнительной классификации по источникам, типам событий реализации риска ИБ и типам потерь, вследствие реализации риска ИБ, в соответствии с пунктом 3 Приложения 2 к настоящему Положению.

7.7. Кредитная организация (головная кредитная организация банковской группы), в целях управления риском ИБ определяет во внутренних документах и обеспечивает функционирование системы обеспечения информационной безопасности, включающей:

стратегию (политику) обеспечения информационной безопасности в соответствии с принятыми государственными стандартами и нормативно правовыми актами Банка России;

организационную структуру обеспечения информационной безопасности, в том числе распределение ролей и обязанностей, исключающее конфликт интересов;

структурное подразделение (его структуру, роли, функционал и полномочия), ответственное за обеспечение информационной безопасности;

должностное лицо, ответственное за функционирование системы информационной безопасности (не ниже члена коллегиального исполнительного органа управления, а также не участвующего в совершении банковских операций и сделок) и организации бухгалтерского и управленческого учета, обеспечения функционирования информационных систем;

критерии оценки эффективности подразделения, ответственного за обеспечение информационной безопасности;

требования к квалификации персонала, в том числе должностного лица, ответственного за функционирование системы информационной безопасности и руководителя подразделения, выполняющих функции по обеспечению информационной безопасности кредитной организации, включая процедуры по аттестации на соответствие их квалификации;

программное обеспечение, технические и специальные аппаратные средства обеспечения информационной безопасности;

процессы обеспечения информационной безопасности и защиты данных;

систему мер обеспечения информационной безопасности и защиты данных;

требования к качеству информационных систем и иных технических средств обеспечения информационной безопасности, а также их классификация по уровням соответствия требованиям;

обеспечение хранения кодов и устройств электронно-цифровой подписи уполномоченных работников кредитной организации, исключающая доступ к ним посторонних лиц и возможность несанкционированного использования;

стресс-тестирование на предмет обеспечения информационной безопасности и обнаружения уязвимостей, результаты которого отражаются в отчете о стресс-тестировании обеспечения информационной безопасности;

независимую оценку на соответствие требованиям обеспечения информационной безопасности, проводимой кредитной организации и(или) приглашенным квалифицированным экспертом.

7.8. Кредитная организация (головная кредитная организация банковской группы), в рамках реализации системы обеспечения информационной безопасности разрабатывает и соблюдает политику информационной безопасности, включающую:

определение ролей и ответственности органов управления;

инструменты и меры обеспечения информационной безопасности и защиты данных;

требования к внешним контрагентам, выполняющим функции обеспечения информационной безопасности (аутсорсинг), а также определение порядка взаимодействия и ответственности между ними;

требования к персоналу кредитной организации в части соблюдения политики информационной безопасности;

требования по обмену информации о событиях риска ИБ и предоставляемых данных Центру мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Главного управления Банка России (далее – ФинЦЕРТ), в соответствии с нормативными актами Банка России;

показатели и методики оценки эффективности обеспечения информационной безопасности и управления риском ИБ;

выполнение требований настоящего Положения.

Политика информационной безопасности утверждается советом директоров (наблюдательным советом) кредитной организации.

Ответственным за соблюдение требований Политики информационной безопасности в кредитной организации является должностное лицо, ответственное за функционирование системы информационной безопасности.

Исполнительный орган управления кредитной организации несет ответственность в целом за соблюдение требований Политики информационной безопасности и настоящего Положения.

7.9. Подразделение, ответственное за информационную безопасность осуществляет следующие функции:

соблюдение мер обеспечения информационной безопасности и защиты информации и иных задач, возложенных на него внутренними документами;

выявление, учет событий, мониторинг риска ИБ, в соответствии с требованиями настоящего Положения;

составление отчетов по обеспечению информационной безопасности и направление их должностному лицу, ответственному за обеспечение информационной безопасности, в службу управления рисками и уполномоченному органу по вопросам информационной безопасности, при его отсутствии коллегиальному исполнительному органу;

разработка, в случае необходимости, рекомендаций по управлению риском ИБ и их направление должностному лицу, ответственному за обеспечение информационной безопасности, руководителям службы

управления рисками, иных структурных подразделений кредитной организации и уполномоченному коллегиальному органу;

координацию и участие в разработке комплекса мер, направленных на снижение уровня риска ИБ в кредитной организации;

направление информации о событиях риска ИБ в ФинЦЕРТ;

мониторинг эффективности управления риском ИБ;

участие в разработке внутренних документов по обеспечению информационной безопасности и управлению риском ИБ;

информирование персонала кредитной организации по вопросам, связанным с управлением риском ИБ;

участие в рамках своей компетенции во взаимодействии кредитной организации с надзорными органами, саморегулируемыми организациями, ассоциациями и участниками финансовых рынков;

иные функции, связанные с обеспечением информационной безопасности и управлением риском ИБ, предусмотренные внутренними документами кредитной организации.

7.10. Внутренняя отчетность кредитной организации по рискам ИБ включает:

информацию о событиях риска ИБ в соответствии с пунктом 4.4. настоящего Положения и контрольных показателей уровня риска ИБ, перечисленных в пункте 2 Приложения 3 к настоящему Положению;

отчеты, в соответствии с требованиями Положения Банка России от 09 июня 2012 года № 382-П «Положение 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» (далее – Положение Банка России № 382-П);

отчеты, в порядке информирования ФинЦЕРТ, в том числе сводные отчеты должностному лицу, ответственному за обеспечение информационной

безопасности и уполномоченному коллегиальному органу о таком информировании.

7.11. Уполномоченное подразделение проводит регулярную (не реже 1 раза в год) независимую оценку, установленных настоящей главой требований.

Глава 8. Требования к управлению риском информационных систем.

8.1. Кредитная организация (головная кредитная организация банковской группы) определяет систему управления риском отказов (нарушения функционирования) применяемых кредитной организацией информационных систем и (или) недостаточности их функциональных возможностей (характеристик) потребностям кредитной организации (далее – риск ИС), включающей мероприятия и процедуры по обеспечению требований к непрерывности, безопасности и качеству функционирования информационных систем с учетом главы 7 настоящего Положения, в соответствии с Федеральным законом от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», ГОСТ Р 53647 «Менеджмент непрерывности бизнеса», ГОСТ Р 57580.1-2017 «Защита информации финансовых организаций», ГОСТ 56939-2016 «Защита информации. Разработка безопасного программного обеспечения», а также с учетом требований к используемым информационным системам, определение которых установлено пунктом 3 статьи 2 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3448; 2010, № 31, ст. 4196; 2011, № 15, ст. 2038; № 30, ст. 4600; 2012, № 31, ст. 4328; 2013, № 14, ст. 1658; № 23, ст. 2870; № 27, ст. 3479; № 52, ст. 6961, ст. 6963; 2014, № 19, ст. 2302; № 30, ст. 4223, ст. 4243; № 48, ст. 6645; 2015, № 1, ст. 84); № 27, ст. 3979; № 29, ст. 4389, ст. 4390; 2016, № 26, ст. 3877; № 28, ст. 4558).

8.2. Для целей управления риском ИС кредитная организация (головная кредитная организация банковской группы) во внутренних документах определяет и соблюдает политику по использованию информационных систем (далее – Политика ИС), как взаимосвязанной совокупности, технических и программных средств, и иных элементов цифровой инфраструктуры, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, в рамках реализации мер поддержки и обеспечения бесперебойности функционирования основных бизнес-процессов кредитной организации (далее – ИС).

8.3. Кредитная организация (головная кредитная организация банковской группы) не реже одного раза в год выносит на рассмотрение исполнительного органа вопрос о пересмотре Политики ИС, в связи с изменением стратегии развития кредитной организации, в зависимости от характера и масштаба осуществляемых операций, действующих бизнес-процессов, изменяющихся факторов внешней среды, результатов процедур управления операционным риском, риском ИБ и ИС, результатов оценки качества функционирования системы управления операционным риском, проведенной уполномоченным подразделением.

8.4. Исполнительный орган управления кредитной организации обеспечивает соблюдение Политики ИС, в том числе определяет:

роли и ответственность структурных подразделений по исполнению Политики;

должностное лицо, ответственное за обеспечение функционирования ИС кредитной организации (далее – должностное лицо, ответственное за ИС);

порядок информационного обмена в рамках реализации Политики ИС;

порядок и периодичность регулярной отчетности должностного лица, ответственного за ИС и подразделений по исполнению Политики ИС перед исполнительным органом кредитной организации.

8.5. Кредитная организация (головная кредитная организация банковской группы) идентифицирует и закрепляет во политике по

использованию ИС перечень основных бизнес-процессов, с выделением в их составе ключевых бизнес-процессов (включая процессы проведения платежей и расчетов, ведения бухгалтерского и управленческого учета, оценки рисков, сохранности данных и конфиденциальной информации, контроля доступа и иных ключевых бизнес-процессов кредитной организации), требующих обеспечения информационного обмена, обработки, хранения и защиты информации посредством реализации ИС.

8.6. Кредитная организация (головная кредитная организация банковской группы) обеспечивает проведение мероприятий, направленных на выявление, оценку, разработку форм (способов) контроля и мер, направленных на снижение уровня риска ИС и сопряженных с ним рисков ИБ, влияющих на ИС (в соответствии с главой 7 настоящего Положения, в том числе, рисков уничтожения (искажения, безвозвратного удаления) носителей и (или) хранилищ информации и данных, хранящихся в ИС).

8.7. Кредитная организация (головная кредитная организация банковской группы), в целях управления рисками ИС разрабатывает и соблюдает требования к ИС, с учетом характера и масштаба влияния на обеспечения функционирования и бесперебойной работы основных бизнес-процессов кредитной организации, включающие:

8.7.1. Требования к структуре ИС:

состав основных функций, компонент, подсистем ИС, и их иерархической структуры в соответствии с заданными функциональными требованиями и техническими заданиями и с учетом требований ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы стадии создания» (утверждено Постановлением Госстандарта СССР от 29.12.1990 № 3469), ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (утверждено Постановлением Госстандарта СССР от 24.03.1989 № 661):

средства и способы обмена и защиты информации между подсистемами ИС, в случае распределенной архитектуры, в том числе с элементами, размещенными у внешних поставщиков услуг и информации (провайдеров, операторов связи или иных контрагентов);

архитектуру взаимодействия со смежными ИС, в том числе третьих лиц и провайдеров.

8.7.2. Требования к стандартизации и унификации, используемые при создании, модернизации и эксплуатации ИС, включающие:

перечень стандартов и ГОСТ, которые соблюдает кредитная организация;

перечень используемых программных и технических средств;

перечень программно-аппаратных решений, требующих лицензирования и сертификации;

разработки (как собственными силами кредитной организации, так и силами привлеченных подрядчиков), приемки и тестирования, сопровождения ИС, включая порядок хранения и изменения исходного кода (в том числе раздельное хранение, исключающее доступ разработчиков), ведение документации и иные требования в соответствии с ГОСТ;

классификацию ИС, с учетом критичности и влияния ИС на ключевые бизнес-процессы, а также влияния сбоев в работе ИС на ключевые бизнес-процессы кредитной организации;

квалификацию и сертификацию персонала, задействованного при разработке и эксплуатации ИС;

закупки услуг и информации, в случаях необходимости привлечения внешних поставщиков услуг, в том числе порядок и правила выбора поставщиков, определения их ответственности и правил взаимодействия.

критерии и порядок определения и оценки технической и экономической целесообразности передачи на аутсорсинг отдельных элементов ИС, включая контроль утраты доступа и (или) контроля кредитной организации за этими элементами ИС и утраты данных.

8.7.3. Требования к надежности функционирования ИС, включающие:

порядок выявления и устранения сбоев в работе ИС, включающий перечень возможных отказов (сбоев ИС) или ее элементов, их классификацию и типовые варианты решения, а также требования к информационному, техническому и программному обеспечению ИС;

перечень показателей надежности функционирования ИС и их пороговые значения;

режимы функционирования ИС (например, период доступности системы в течении суток, максимальное допустимое время простоя в год, допустимые интервалы в случаи установки обновления и другие);

инструменты, методы контроля и способы оценки надежности функционирования ИС кредитной организации;

требования к аутсорсингу обслуживания и функционирования ИС, включая обязательные меры обеспечения сохранности, доступа и контроля кредитной организации за элементами ИС, переданных на аутсорсинг, в том числе персональной ответственности должностных лиц за сохранность ИС и данных, переданных на аутсорсинг;

меры по повышению качества функционирования ИС;

период коммерческого использования с сохранением требуемых функций ИС (жизненный цикл ИС);

иные требования, отражающие особенности обеспечения функционирования ключевых бизнес-процессов и структуры ИС кредитной организации.

8.7.4. Требования к обеспечению качества данных, в разрезе характеристик качества данных, определенных в соответствии с абзацами 2-8 пункта 1 Приложения 3 Положения Банка России от 06.08.2015 № 483-П «О порядке расчета величины кредитного риска на основе внутренних рейтингов»:

точности и достоверность данных;

полноты данных;

актуальности данных;

согласованности данных;

доступности данных;

контролируемости данных;

восстанавливаемости данных;

иные характеристики качества данных, определяемые кредитной организацией самостоятельно (при необходимости).

Кредитная организация (головная кредитная организация банковской группы), с учетом характера и масштаба осуществляемых операций, уровня и сочетания принимаемых рисков, действующих бизнес-процессов, текущих и стратегических планов развития и доступных возможностей может самостоятельно определить во внутренних документах дополнительные характеристики качества и иные требования к качеству данных, например, указанных в пунктах 2-3 Приложения 3 Положения Банка России от 06.08.2015 № 483-П «О порядке расчета величины кредитного риска на основе внутренних рейтингов», включая их классификацию, характеристики, инструменты, методы и средства контроля.

8.7.5. Кредитная организация (головная кредитная организация банковской группы) может самостоятельно определить во внутренних документах дополнительные требования к ИС и их функционированию с учетом характера и масштаба осуществляемых операций, уровня и сочетания принимаемых рисков, основных действующих бизнес-процессов, текущих и стратегических планов развития и доступных возможностей.

8.7.6. Кредитная организация (головная кредитная организация банковской группы) не реже одного раза в год пересматривает требования к ИС с учетом текущих и стратегических планов развития, а также оценки уровня операционного риска и их влияния на ключевые бизнес-процессы, отраженной во внутренней отчетности по операционному риску и мер, направленных на снижение уровня операционного риска, внутренней

отчетности подразделения, ответственного за обеспечение информационной безопасности и подразделения, ответственного за работу ИС.

8.8. Кредитная организация (головная кредитная организация банковской группы) разрабатывает, соблюдает и отражает во внутренних документах требования по обеспечению непрерывности, безопасности и качества функционирования ИС, включающие:

8.8.1. Разработку, реализацию и контроль выполнения требований к обеспечению, разработке, модернизации и эксплуатации ИС в соответствии с главой 7 настоящего Положения.

8.8.2 Обеспечение технических условий эксплуатации технических средств ключевых элементов ИС, включая устройства бесперебойного электропитания, вентиляции и кондиционирования, резервные цифровые каналы и устройств связи, резервные носители данных.

8.8.3 Регулярное (не реже одного раза в день) резервное копирование данных ключевых бизнес процессов на резервные технические средства, размещенные в иных зданиях чем те, в которых размещены действующие технические средства, обеспечивающие функционирование ИС в текущем рабочем режиме. Кредитная организация обеспечивает надежность функционирования резервных технических средств, в том числе требования пункта 8.8.2 настоящего Положения, режим охраны и доступа.

8.8.4 Использование лицензионного и сертифицированного программного обеспечения, то есть приятого в эксплуатацию с соблюдением требований пункта 8.7.2 настоящего Положения, с соблюдением технических условий эксплуатации, описанных в эксплуатационной документации программного обеспечения.

8.8.5. Наличие во внутренних документах кредитной организации положения и стратегии по обеспечению непрерывности и восстановления функционирования ИС;

8.8.6. Проведение кредитной организацией регулярных (не реже 1 раза в год) оценок состава компонент, архитектуры, инфраструктуры и

характеристик ИС на их достаточность и эффективность для обеспечения функционирования ключевых бизнес-процессов кредитной организации, по результатам которых принимаются меры по устранению выявленных недостатков в ИС.

8.8.7. Ежегодное тестирование и анализ уязвимостей ИС или их компонент, в том числе разработку комплекса мер, направленных на устранение выявленных уязвимостей.

8.8.8. Проведение уполномоченным подразделением регулярной (не реже 1 раза в год) независимой оценки, установленных настоящей главой требований, включающих оценку качества:

соблюдения Политики ИС;

мероприятий, направленных на выявление, регулирование, разработку мер, направленных на снижение риска ИС и сопряженных с ними рисков ИБ, влияющих на ИС;

требований к ИС в целях управления рисками ИС и их соблюдения;

требования по обеспечению непрерывности, безопасности и качества функционирования ИС.

Уполномоченное подразделение направляет отчеты по результатам оценки исполнительному органу кредитной организации, подразделениям, ответственным за обеспечение функционирования ИС и службе управления рисками.

8.8.9. Кредитная организация (головная кредитная организация банковской группы) определяет подразделение (одно или несколько), ответственное за обеспечение непрерывности функционирования ИС, в зоне ответственности которого находятся ИС, включая:

определение ролей, ответственности, полномочий подразделения (и его сотрудников);

целевые показатели и критерии эффективности работы подразделения, с занесением их в положения о подразделении (и должностные инструкции сотрудников);

контрольные процедуры и целевые показатели, включая порядок их актуализации;

8.8.10. Кредитная организация (головная кредитная организация банковской группы) определяет должностное лицо, ответственное за обеспечение непрерывности функционирования ИС в кредитной организации, включая его полномочия и требования к его квалификации и сертификации (при необходимости);

8.8.11. Кредитная организация (головная кредитная организация банковской группы) проводит самооценку рисков ИС в разрезе бизнес-процессов и соблюдения требований настоящей главы, и направляет отчеты по результатам самооценки в подразделение, ответственное за управление операционным риском и(или) иному уполномоченному органу.

8.8.12. Внутренняя отчетность кредитной организации по риску информационных систем включает:

информацию о сбоях ИС;

информацию о событиях риска ИС в соответствии с пунктом 4.2 настоящего Положения;

отчеты по результатам самооценки риска ИС в разрезе бизнес-процессов, в том числе ключевых, структурных подразделений кредитной организации, категорий ИС.

8.8.13. Кредитная организация (головная кредитная организация банковской группы) может самостоятельно определять дополнительные требования к обеспечению постоянного функционирования ИС, безопасности и качеству функционирования ИС, с учетом характера и масштаба осуществляемых операций, принимаемых рисков, действующих бизнес-процессов, текущих и стратегических планов развития, доступных возможностей может самостоятельно определить во внутренних документах.

Глава 9. Порядок надзорной оценки системы управления операционным риском.

9.1. Структурное подразделение Банка России, уполномоченное осуществлять надзор за кредитными организациями (далее – уполномоченное структурное подразделение Банка России) ежегодно оценивает систему управления операционным риском, включая систему управления рисками ИБ и ИС, а также соблюдения кредитной организацией требований к ИС (далее – оценка системы управления операционным риском).

9.2. В случае если в рамках оценки системы управления операционным риском выявляется несоответствие системы управления операционным риском в кредитной организации требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности, то уполномоченное структурное подразделение Банка России совершает действия, указанные в пунктах 9.6 и 9.7 настоящего Положения, не позднее 5 календарных дней с момента возникновения соответствующих оснований.

9.3. При оценке системы управления операционным риском, уполномоченное структурное подразделение Банка России рассматривает следующие документы:

политики управления операционным риском, риском ИБ и ИС;

внутренние документы по управлению операционным риском, риском ИБ и ИС (положения, порядки, методики, инструкции и иные документы), включая приказы и распоряжения руководителей кредитной организации о вводе этих документов в действие и указанием лиц ответственных за их исполнение;

техническая и иная документация о базе событий операционного риска, риска ИБ и ИС, а также иных систем, используемых в системе управления операционным риском, риском ИБ и ИС;

письменных уведомлений, содержащих информацию о назначении (освобождении от занимаемой должности) лиц, исполняющих функции

должностного лица, ответственного за управление рисками, должностного лица, ответственного за обеспечение информационной безопасности, должностного лица, ответственного за обеспечение работы ИС кредитной организации, руководителей структурных подразделений, ответственных за управление операционным риском, риском ИБ, о соответствии указанных лиц квалификационным требованиям и требованиям к деловой репутации, направляемых в соответствии с требованиями Банка России;

положения о подразделениях по управлению операционным риском, риском ИБ и обеспечения функционирования ИС;

должностные инструкции сотрудников и руководителей структурных подразделений кредитной организации, ответственных за управление операционным риском, отвечающих за обеспечение ИБ и обеспечение функционирования ИС;

документы о проведении мероприятий по выявлению операционного риска и результатам этих мероприятий;

документы по расчетам контрольных показателей уровня операционного риска и риска ИБ;

внутреннюю отчетность по операционному риску, включающую докладные записки, мотивированные суждения по предложениям о мерах, направленных на снижение уровня операционного риска и иные документы, подготовленные подразделениями, ответственными за управление операционным риском, риском ИБ и обеспечения функционирования ИС, о состоянии системы управления операционным риском, включая риски ИБ и ИС;

протоколы заседаний исполнительного органа кредитной организации о рассмотрении внутренней отчетности по операционным рискам кредитной организации, а также результатов оценки качества функционирования систем управления операционным риском, риском ИБ и ИС, иных документов, описывающих состояние системы управления операционным риском, риском ИБ и ИС, и принятыми решениями;

отчеты о результатах оценки качества функционирования системы управления операционным риском (включая риск ИБ и ИС), проведенной уполномоченным подразделением, подготовленные для рассмотрения исполнительным органом кредитной организации;

отчеты внешних экспертов о результатах оценки системы управления операционным риском, риском ИБ и ИС;

протоколы заседаний совета директоров (наблюдательного совета) кредитной организации по вопросам системы управления операционным риском, риском ИБ и ИС;

выгрузки базы событий операционного риска, риска ИБ и ИС;

выгрузки из автоматизированной банковской системы кредитной организации по счетам расходов бухгалтерского учета для учета потерь от операционного риска, риска ИБ и ИС;

В целях оценки кредитной организации уполномоченное структурное подразделение Банка России, вправе запрашивать у кредитной организации дополнительную информацию по вопросам организации системы управления операционным риском в кредитной организации, в том числе деятельности подразделения, ответственного за управление операционным риском (ее руководителя) и подразделения, ответственного за обеспечение информационной безопасности (ее руководителя).

9.4. При проведении оценки системы управления операционным риском может осуществляться оценка как системы управления операционным риском в целом, так и отдельных их элементов, в том числе операций (процедур) на предмет получения подтверждения:

соблюдения внутренних методик и процедур, а также установленных требований;

достоверности, полноты и объективности систем учета и отчетности, сбора, обработки и хранения данных по событиям операционного риска и риска ИБ;

эффективности установленных и применяемых кредитной организацией способов, методов оценки и контроля операционных рисков, а также мер, направленных на снижение уровня операционного риска и (или) снижения последствий, в случае реализации события операционного риска.

9.5. Кредитная организация (головная кредитная организация банковской группы) обязана представить по запросу уполномоченного структурного подразделения Банка России копии указанных в пункте 9.3. настоящего Положения документов (при их отсутствии) в течение 10 рабочих дней со дня получения кредитной организацией такого запроса.

Запрос направляется руководителем (заместителем руководителя) уполномоченного структурного подразделения Банка России либо лицами, их замещающими.

Запрос не направляется, если указанные в настоящем пункте документы были представлены в уполномоченное структурное подразделение Банка России в текущем календарном году и имеется письменное подтверждение кредитной организации, что в них не вносились изменения.

Банк России обеспечивает конфиденциальность поступившей от кредитных организаций информации об их системах управления операционным риском.

9.6. Уполномоченное структурное подразделение Банка России направляет в кредитную организацию информацию о несоответствии ее системы управления операционным риском требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности.

Кредитная организация (головная кредитная организация банковской группы) в случае несогласия с несоответствием системы управления операционным риском требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности имеет право представить в уполномоченное структурное подразделение Банка России мотивированное возражение в течение 10

рабочих дней со дня получения кредитной организацией информации об оценке кредитной организации.

Уполномоченное структурное подразделение Банка России обязано рассмотреть мотивированное возражение кредитной организации в срок не более 10 рабочих дней со дня его получения.

9.7. В случае если кредитная организация (головная кредитная организация банковской группы) не направила в уполномоченное структурное подразделение Банка России мотивированное возражение в срок, установленный пунктом 9.6 настоящего Положения, либо по результатам рассмотрения направленного кредитной организацией мотивированного возражения уполномоченным структурным подразделением Банка России не изменена оценка кредитной организации о несоответствии системы управления операционным риском в кредитной организации требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности, уполномоченное структурное подразделение Банка России не позднее 30 рабочих дней с даты направления в кредитную организацию информации о несоответствии системы управления операционным риском в кредитной организации требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности, направляет в кредитную организацию предписание об устранении соответствующего нарушения.

9.8. В случае неисполнения в установленный уполномоченным структурным подразделением Банка России срок предписания Банка России об устранении нарушений, выявленных в системе управления операционным риском кредитной организации, Банк России вправе применять к такой кредитной организации меры, установленные статьей 74 Федерального закона «О Центральном банке Российской Федерации (Банке России)».

Глава 10. Заключительные положения.

10.1. Настоящее Положение вступает в силу по истечении 10 дней после дня его официального опубликования.

10.2. Кредитным организациям (головным кредитным организациям банковской группы) привести систему управления операционным риском в соответствие настоящему Положению в срок до 31 декабря 2019 года.

10.3. Оценка Банком России соответствия системы управления операционным риском в кредитной организации требованиям настоящего Положения, с учетом характера и масштаба совершаемых ею операций, результатам ее деятельности, в соответствии с главой 9 настоящего Положения проводится, начиная с 1 января 2020 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение 1
к Положению Банка России
от «___»_____ 201__ № _____-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Классификация
типов событий операционного риска второго уровня.

Кредитные организации для целей управления операционным риском классифицируют события операционного риска по типам событий дополнительной детализации в разрезе основной классификации типов событий:

1. Тип события «внутреннее мошенничество», включающий:

1.1. неразрешенная деятельность, состоящая в преднамеренных действиях работников, связанные с сознательным превышением работниками своих полномочий при проведении или одобрении сделки (осуществлении операций), закрепленных должностными инструкциями, внутренними нормативными документами или решениями органов управления кредитной организации, без цели присвоения имущества, материальных и(или) нематериальных активов, но в целях получения иной выгоды. К данному типу событий не относятся непреднамеренные ошибки сотрудников, являющиеся следствием несовершенства внутренних процессов, продуктов или противоречий во внутренних документах;

1.2. Кражи и мошенничество, состоящие в противоправных действиях работников в отношении имущества, материальных и(или) нематериальных активов кредитной организации и средств клиентов, с целью их присвоения (уничтожения, хищения) для целей личной выгоды, в то числе с использованием коммерческого подкупа (коррупции).

2. Тип события «внешнее мошенничество», включающий:

2.1. Кражи и мошенничества, состоящие в противоправных действиях третьих лиц, в отношении имущества, материальных и(или) нематериальных активов кредитной организации и средств клиентов. К данному типу событий не относятся события киберриска.

2.2. Нарушение безопасности информационных систем, состоящее в преднамеренных действиях третьих лиц в отношении имущества, информации, данных, материальных и(или) нематериальных активов кредитной организации и средств клиентов. К данному типу событий относятся все виды электронного мошенничества совершенного третьими лицами с применением средств цифровой инфраструктуры (реализации событий киберриска) по отношению к информации, данным, содержащимся во внутренних ИС банка;

3. Тип события «нарушения кадровой политики и безопасности труда», включающий:

3.1. Нарушение трудового законодательства, состоящее в нарушении со стороны кредитной организации норм трудового законодательства, результатом которого стали выплаты работникам (или бывшим работниками) в виде компенсаций за нарушение условий трудового договор и(или) административных штрафов надзорным органам по вопросам применения трудового законодательства.

3.2. Нарушение норм безопасности и охраны труда, состоящее в нарушении кредитной организацией норм безопасности и охраны труда, результатом которых стали выплаты работникам (или бывшим работникам) компенсаций за причинение ущерба здоровью и(или) административных штрафов надзорным органам по вопросам безопасности и охраны труда.

3.3. Дискриминация. К данному типу событий относятся все нарушения прав работников и третьих лиц, связанных с дискриминацией (половая, расовая, национальная дискриминация, а также по языку, происхождению,

имущественному и должностному положению, месту жительства, отношению к религии, убеждениям, принадлежности к общественным объединениям).

4. Тип события «нарушения прав клиентов и нанесения им ущерба», включающий:

4.1. Нарушения прав клиентов, состоящие в действиях со стороны кредитной организации, которые привели к раскрытию конфиденциальной информации, нарушению информационного обмена и взаимодействию с клиентом, повлекшие нарушение интересов клиентов и выплаты клиентам компенсаций.

4.2. Нарушение норм делового оборота и рыночных практик, состоящее в нарушении кредитной организацией гражданского законодательства, условий договоров на совершение банковских операций, стандартов поведения на финансовых рынках, предоставления банковских услуг, внутренних процедур кредитной организации взаимодействия с клиентами и контрагентами.

4.3. Недостатки банковских услуг и операций, состоящие в нарушении кредитной организации интересов и прав клиентов вследствие свойств, сложившейся в кредитной организации практики оказания услуг и операций, рекламы, навязывания сопутствующих услуг. К данному типу событий не относятся события, произошедшие в результате недостатка внутренних процессов.

4.4. Нарушение требований изучения клиентов, состоящее в нарушении требований законодательства в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, результатом которых стали административные штрафы и предписания надзорных органов.

4.5. Недостатки в работе с контрагентами, связанные с негативными событиями у контрагентов (поставщиков услуг) по вине кредитной организации, результатом которых стали претензии контрагентов и выплата им компенсаций.

5. Тип события «ущерб материальным (физическим) активам», включающий события стихийного характера и прочие внешние события (форс-мажоры), в том числе природные, техногенные, социальные, медико-биологические катастрофы, повлекшие досрочное списание (полное или частичное выбытие) материальных и(или) нематериальных активов кредитной организации.

6. Тип события «нарушения функционирования и сбои систем», включающий:

6.1. Сбои в работе информационных систем и программного обеспечения, связанные с нарушением работоспособности технических средств и оборудования, цифровой инфраструктуры, программного обеспечения и иных элементов информационных систем кредитной организации.

6.2. Инфраструктурные сбои, состоящие в нарушении работы инфраструктуры (сбой системы кондиционирования, водоснабжения, электроснабжения) за исключением сбоев информационных систем и цифровой инфраструктуры, оказавшем влияние на деятельность кредитной организации. К данному типу событий относятся события, связанные с нарушением работы;

7. Тип события «нарушения при организации, исполнении и управлении процессами», включающий:

7.1. Ошибки при подготовке, проведении и сопровождении банковских операций, состоящие в нарушении внутренних процедур, стандартов, правил кредитной организации, например к данному типу событий относятся события непреднамеренного характера, связанные с нарушением внутренних процедур проведения операций работниками кредитной организации (не связанные с внутренним мошенничеством), события, связанные с несовершенством (недостатками) внутренних процессов, системы внутреннего контроля, управления рисками, недостатков распределения ролей и полномочий, ошибок корпоративного управления;

7.2. Ошибки во внутренних процессах бухгалтерского и аналитического учета и отчетности, состоящие в нарушении правил и сроков соблюдения бухгалтерского учета и предоставления иной обязательной отчетности.

7.3. Ошибки при подготовке договоров и документационного обмена, состоящие в ошибках при работе с клиентской документацией, документообороте, информационном обмене кредитной организации с клиентами.

7.4. Ошибки расчетно-кассового обслуживания и управления счетами клиентов, состоящие в нарушении порядка работы со счетами клиентов, в том числе нарушения работы со средствами клиентов, находящимся в доверительном управлении;

7.5. Недостатки работы с контрагентами, выбора поставщиков услуг. К данному типу событий относятся события, связанные с потерями кредитной организации, возникшими в результате работы контрагентов (поставщиков услуг), зависимости процессов кредитной организации от поставщиков и провайдеров услуг;

7.6. Ошибки кредитной организации, связанные с несоответствием документов кредитной организации действующему законодательству, нормативным документам надзорных органов.

Приложение 2
к Положению Банка России
от «___»_____ 201__ № _____-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Подходы к дополнительной классификации риска ИБ.

1. Риск ИБ дополнительно классифицируется по событиям в разрезе типов событий в соответствии с пунктом 2.7.7 настоящего Положения и трех видов нарушения защиты информации:

1.1. События киберриска, связанные с переводами денежных средств в значении, установленном в соответствии с Федеральным законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», и приводящие к следующим последствиям:

к использованию электронных средств платежа клиентов кредитных организаций без их согласия;

к несанкционированному доступу к объектам информационной инфраструктуры кредитной организации, приведшие к несанкционированным переводам и снятиям денежных средств;

списаниям денежных средств с корреспондентских счетов кредитных организаций и (или) с использованием искаженной информации, содержащейся в распоряжениях о переводе денежных средств;

неоказанию кредитной организацией услуг по переводу денежных средств;

иные преднамеренные нарушения и недостатки обеспечения информационной безопасности в кредитной организации и управления рисками ИБ при осуществлении переводов и платежей.

1.2. События киберриска, не связанные с переводами денежных средств, возникшие в результате несанкционированного доступа и (или) реализации

компьютерных атак к объектам информационной инфраструктуры и (или) информационным системам, и приводящие к следующим последствиям:

несанкционированный доступ к объектам информационной инфраструктуры, данным и (или) информационным системам кредитной организации;

реализация атак на информационную инфраструктуру и (или) информационные системы кредитной организации типа «отказ в обслуживании» (DDOS-атаки), предпринимаемых с целью блокирования нормального функционирования информационной инфраструктуры и (или) информационных систем кредитной организации;

воздействие компьютерных вирусов на информационную инфраструктуру и (или) информационные системы кредитной организации;

создание и эксплуатация уязвимостей в программном обеспечении информационных систем кредитной организации;

создание и эксплуатация уязвимостей элементов инфраструктуры и (или) технологических систем;

создание и эксплуатация уязвимостей систем жизнеобеспечения и (или) контроля доступа;

иные нарушения и недостатки обеспечения информационной безопасности и управления рисками информационной безопасности на объектах информационной инфраструктуры и (или) информационных системах кредитной организации.

1.3. События, связанные с обработкой (хранением, уничтожением) информации без использования средств цифровой инфраструктуры и приводящие к следующим последствиям:

утечке, искажению или потери конфиденциальной информации кредитной организации;

копированием конфиденциальных данных сотрудниками компании;

хищению или утратой носителей информации кредитной организации.

2. По дополнительным (специфическим) источникам риска ИБ (угрозам, уязвимостям), в разрезе категорий источников операционного риска, приведенных в главе 2 настоящего Положения.

2.1. По категории источников риска в соответствии с пунктом 2.3.1 настоящего Положения:

нарушения операторами платежных систем, операторами услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных в нормативных актах Банка России, разработанных в соответствии с Положением Банка России от 24 августа 2016 года № 552-П «О требованиях к защите информации в платежных системах» (далее – Положение Банка России № 552-П);

нарушения участниками платежной системы Банка России требований к защите информации при осуществлении переводов денежных средств в платежной системе Банка России, установленных в нормативных актах Банка России, разработанных в соответствии с Положением Банка России № 382-П;

уязвимости кода (уязвимости, появившиеся в процессе разработки программного обеспечения);

уязвимости конфигурации (уязвимости, появившиеся в процессе задания конфигурации (применения параметров настройки) программного обеспечения и технических средств информационной системы);

уязвимости информационной архитектуры (уязвимости, появившиеся в процессе проектирования информационной системы);

организационные уязвимости (уязвимости, появившиеся в связи с отсутствием (или недостатками) организационных мер защиты информации в информационной системе и (или) несоблюдением правил эксплуатации системы защиты информации в информационной системе);

иные недостатки внутренних процессов, обеспечивающих функционирование информационной инфраструктуры кредитной организации и систем защиты информации, нарушения требований

национальных стандартов Российской Федерации, разрабатываемых Банком России в рамках законодательства Российской Федерации о техническом регулировании и стандартизации, обязанность применения которых установлена в нормативных актах Банка России.

2.2 По категории источников риска в соответствии с пунктом 2.3.2 настоящего Положения:

события риска ИБ с использованием легально предоставленных им прав логического или физического доступа;

события риска ИБ без использования легально предоставленных прав логического или физического доступа.

2.3. По категории источников риска в соответствии с пунктом 2.3.3 настоящего Положения:

сбои и отказы в работе программного обеспечения специальных средств и систем защиты данных информационной инфраструктуры и (или) информационных систем кредитной организации;

сбои и отказы в работе программного обеспечения и (или) систем контроля доступа;

2.4. По категории источников риска в соответствии с пунктом 2.3.4 настоящего Положения:

воздействия со стороны третьих лиц или информационных систем с целью блокирования штатного функционирования бизнес-процессов или технологических процессов кредитной организации;

воздействия со стороны третьих лиц или информационных систем с целью хищения, искажения, удаления информации конфиденциального характера (включая персональные данные), информации ограниченного доступа и иных типов информации кредитной организации, не подлежащей разглашению или опубликованию.

2.5. Следующие уровни классификации источников (угроз, уязвимостей) событий риска ИБ определяются по видам процессов обеспечения мер информационной безопасности в соответствии с пунктом 2.1 к настоящему

Приложению, в зависимости от процессов кредитной организации, в которых они произошли.

В случае, если в процессе анализа риска ИБ выявляются иные источники возникновения события риска ИБ кредитная организация в базе событий операционного риска определяет эти источники.

3. Кредитные организации используют дополнительные (специфические) типы прямых и непрямых потерь от реализации рисков ИБ для классификации событий, в дополнение к пункту 2.11 настоящего Положения.

3.1. По категории «прямые потери» события риска ИБ классифицируются следующим образом:

потери денежных средств или иных активов кредитной организации, в результате реализации рисков ИБ, указанных в пункте 1.1 настоящего Приложения;

выплаты компенсаций клиентам и контрагентам, в результате реализации рисков ИБ, указанных в пункте 1 настоящего Приложения;

уплата штрафов по предписаниям регуляторов и (или) администраторов платежных систем за реализацию риска ИБ.

3.2. По категории «косвенные потери»:

расчетные потери из-за простоев информационной инфраструктуры или потери ее работоспособности в результате реализации рисков ИБ, указанных в пункте 1.1 настоящего Приложения;

рост затрат рабочего времени обслуживающего персонала на устранение последствий от реализации риска ИБ;

рост стоимости договоров технического обслуживания информационной инфраструктуры и (или) антивирусной защиты.

3.3. По категории «качественные потери»:

простои бизнес процессов;

потеря работоспособности информационной инфраструктуры;

искажение программного кода;

искажение или потеря данных;

возникновение иных уязвимостей в информационной инфраструктуре;

перегрузка вычислительных мощностей и трафика электронных каналов связи не штатными операциями;

иные потери качества информационной инфраструктуры.

3.4. Кредитная организация (головная кредитная организация банковской группы) обеспечивает выявление, регистрацию и учет всех событий реализации риска ИБ, с определением всех классификационных признаков в соответствии с главами 2 и 6 настоящего Положения, Приложениями 1 и 2 к настоящему Положению, классифицирует суммы и величины потерь в разрезе классификационных признаков, в соответствии с пунктами 2.11 настоящего Положения и пункта 3 настоящего Приложения, с распределением по датам отражения в бухгалтерском учете, с раздельным учетом поступивших возмещений (компенсаций).

Приложение 3
к Положению Банка России
от «___»_____ 201__ № _____-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Рекомендуемый перечень возможных мер, направленных на снижение уровня операционного риска.

Кредитная организация может использовать, но не ограничиваться следующим перечнем возможных мер, направленных на снижение уровня операционного риска.

1.1.Регламентация, в том числе своевременная актуализация, процессов проведения банковских операций (сделок) с соблюдением действующего законодательства;

1.2. Применение стандартизированных (типовых) форм внутренних документов кредитной организации

1.3. Стандартизация типовых операций (сделок);

1.4. Применение типовых форм договоров с клиентами (контрагентами);

1.5. Контроль (автоматизированный, ручной) за соблюдением внутренних документов кредитной организации;

1.6. Подбор и аттестация персонала;

1.7. Разработка системы мотивации персонала;

1.8. Проведение тренингов и обучение персонала проведению сделок (операций);

1.9. Процедура коллегиального принятия решений, например, по проведению крупных сделок (нестандартных сделок);

1.10. Особый контроль за проведением крупных сделок (нестандартных сделок);

1.11. Контроль сделок (операций);

1.12. Отчетность по сделкам (операциям);

1.13. Тестирование бизнес-процессов, технологических, информационных систем кредитной организации;

1.14. Автоматизация бизнес-процессов (операций), алгоритмизация типовых сделок (операций);

1.15. Проверка документов, в том числе первичных, по проводимым сделкам (операциям);

1.16. Разграничение ролей, ответственности и полномочий персонала при проведении сделок (операций);

1.17. Использование двойного контроля при проведении сделок (операций);

1.18. Установление и контроль соблюдения лимитов при проведении сделок (операций);

1.19. Установление и разделение прав доступа к информации и ИС;

1.20. Резервирование информации в ИС;

1.21. Установление и разделение прав доступа к использованию материальных и нематериальных активов;

1.22. Организация физической безопасности объектов и материальных активов кредитной организации;

1.23. Идентификационные процедуры клиентов, контрагентов, конечных бенефициаров, представителей клиентов, выгодоприобретателей и изучение сделок (операций) клиентов;

1.24. Противодействие неправомерному использованию инсайдерской информации;

1.25.Контроль качества данных в бизнес-процессах, ИС;

1.26. Процедуры ограничения на ввод данных в ИС;

1.27. Автоматические сверки контроля вводимых данных в ИС;

1.28. Контроль сроков и рассылка уведомлений участникам бизнес-процессов;

1.29. Автоматический контроль маршрута согласований сделок (операций);

1.30. Мероприятия по повышению культуры управления рисками;

1.31. Система ключевых показателей деятельности, стимулирующая персонал эффективно управлять рисками;

1.32. иные меры, направленные на снижение уровня операционного риска.

Приложение 4
к Положению Банка России
от «___»_____ 201__ № _____-П
«О требованиях к системе управления
операционным риском в кредитной
организации и банковской группе»

Контрольные показатели уровня операционного риска
и риска ИБ.

1. Кредитная организация (головная кредитная организация банковской группы) определяет порядок установления и контроля соблюдения следующих контрольных показателей уровня операционного риска в соответствии с главой 5 настоящего Положения.

1.1. Базовый набор показателей системы управления операционными рисками.

1.1.1. Для кредитных организаций, применяющих регуляторный подход к расчету необходимого капитала для покрытия операционного риска:

общая сумма валовых прямых потерь понесенных кредитной организации от реализации событий операционного риска за вычетом потерь от событий риска ИБ за определенный период (наращенным итогом за 3, 6, 9 месяцев и год);

отношение общей суммы валовых прямых потерь от реализации событий операционного риска за вычетом потерь от событий риска ИБ, понесенных кредитной организацией за годовой период к базовому капиталу кредитной организации на последнюю отчетную дату года;

отношение общей суммы валовых прямых потерь от реализации событий операционного риска за вычетом потерь от событий риска ИБ, к показателю Д, рассчитанному в соответствии с положением Банка России от 03.11.2009 № 346-П «О порядке расчета операционного риска» (далее – Положение Банка России № 346-П) на последнюю отчетную дату;

отношение суммы чистых прямых потерь от реализации событий операционного риска (в соответствии с главой 6 настоящего Положения) за вычетом потерь от событий риска ИБ, к показателю Д, рассчитанному в соответствии с Положением Банка России № 346-П на последнюю отчетную дату;

доля выявленных в ходе оценки качества функционирования системы управления операционного риска, проведенной уполномоченным подразделением, внешним экспертом, или Банком России событий операционного риска с ненулевыми прямыми потерями (за исключением потерь от кредитного риска), которые кредитная организация не отразила в базе событий, по отношению ко всем зарегистрированным в базе событий событиям операционного риска с ненулевыми прямыми потерями (за исключением потерь от кредитного риска) за годовой период, к которому относится проверяемый период (контрольное лимитное значение должно быть не больше 1%, сигнальное значение – не больше 0,5%);

отношение сумм валовых прямых потерь от выявленных в ходе оценки качества функционирования системы управления операционного риска, проведенной уполномоченным подразделением, внешним экспертом, или Банком России событий операционного риска с ненулевыми потерями (за исключением потерь от кредитного риска), которые кредитная организация не отразила в базе событий к общей сумме валовых прямых потерь всех зарегистрированных в базе событий операционного риска с ненулевыми прямыми потерями (за исключением потерь от кредитного риска), в соответствии с за годовой период, к которому относится проверяемый период (контрольное лимитное значение должно быть не больше 1%, сигнальное значение – не больше 0,5%);

иные количественные показатели, определяемые кредитной организацией самостоятельно в стратегии управления рисками и капиталом.

1.1.2. Кредитные организации, применяющие продвинутый подход к расчету необходимого капитала на покрытие операционного риска, кроме

базовых показателей, перечисленных в пункте 1.1.1 настоящего Приложения, используют следующие дополнительные показатели:

прямые и косвенные потери, определяемых расчетным образом, от реализации событий операционного риска за определенный период (наращенным итогом за 3, 6, 9 месяцев и год) за вычетом потерь от событий риска ИБ;

отношение прямых и косвенных потерь, определяемых расчетным образом, от реализации событий операционного риска за вычетом потерь от событий риска ИБ, понесенных кредитной организацией за годовой период к общему капиталу (собственным средствам) кредитной организации на последнюю отчетную дату года.

1.2. К качественным контрольным показателям уровня операционного риска относятся, качественные оценки по четырехуровневой системе («хорошо», «удовлетворительно», «сомнительно», «неудовлетворительно») по следующим направлениям:

оценка качества функционирования системы управления операционного риска, проведенная уполномоченным подразделением, в соответствии с пунктом 4.4. настоящего Положения;

оценка системы управления операционным риском, проведенная в рамках оценки качества систем управления рисками и капиталом в соответствии с Указание Банка России от 7 декабря 2015 года № 3883-У «О порядке проведения Банком России оценки качества систем управления рисками и капиталом, достаточности капитала кредитной организации и банковской группы»;

иные качественные показатели, определяемые кредитной организацией самостоятельно в стратегии управления рисками и капиталом.

1.3. Исполнительный орган кредитной организации определяет лимиты операционного риска на основе установленных в политике управления операционным риском значений уровней контрольных показателей уровня операционного риска путем их распределения по направлениям деятельности

(бизнес-процессам), структурным подразделениям, источникам, видам операционного риска, типам событий и видам потерь, на основе пункта 1.1.1 настоящего Приложения.

2. Базовый набор показателей системы управления риском ИБ.

2.1. Количественные показатели системы управления риском ИБ:

2.1.1. Для кредитных организаций, применяющих регуляторный подход к расчету необходимого капитала для покрытия операционного риска:

прямые потери от реализации событий риска ИБ за определенный период (наращенным итогом за 3, 6, 9 месяцев и год);

прямые потери от реализации событий риска ИБ, связанные с переводами денежных средств и платежами в платежных системах, в соответствии пунктом 1.1. Приложения 2 к настоящему Положению, за определенный период (наращенным итогом за 3, 6, 9 месяцев и год);

отношение общей суммы прямых потерь от событий риска ИБ, понесенных кредитной организации за годовой период к базовому капиталу кредитной организации на последнюю отчетную дату года;

отношение суммы прямых потерь, понесенных кредитной организации за определенный период (наращенным итогом за 3, 6, 9 месяцев и год) при выполнении кредитной организацией функций участника платежной системы Банка России к общей сумме операций по переводу денежных средств через платежную систему Банка России за этот же период (контрольное лимитное значение должно быть не больше 0,05%, сигнальное значение – не больше 0,005%);

отношение суммы прямых потерь от реализации событий риска ИБ, связанных с переводами денежных средств и платежами в платежных системах, в соответствии пунктом 1.1. Приложения 2 к настоящему Положению, за определенный период (наращенным итогом за 3, 6, 9 месяцев и год) к общей сумме переводов денежных средств и платежами в платежных системах за этот же период (контрольное лимитное значение должно быть не больше 0,05%, сигнальное значение – не больше 0,005%);

отношение суммы денежных средств, по которой получены уведомления клиентов о несанкционированном переводе (списании) денежных средств, за определенный период (наращенным итогом за 3, 6, 9 месяцев и год) к общей сумме переводов за этот же период (контрольное лимитное значение должно быть не больше 0,05%, сигнальное значение – не больше 0,005%);

доля реализованных, то есть не предотвращенных системой информационной безопасности кредитной организации, событий риска ИБ с ненулевой величиной прямых потерь по отношению ко всем зарегистрированным событиям риска ИБ с ненулевой величиной прямых потерь в течение отчётного периода, о которых кредитная организация сообщила в своих отчетах в ФинЦЕРТ;

доля выявленных в ходе оценки качества функционирования системы управления операционного риска, проведенной уполномоченным подразделением, внешним экспертом, или Банком России событий рисков ИБ с ненулевой величиной прямых потерь, о которых кредитная организация не сообщила в своих отчетах в ФинЦЕРТ, по отношению ко всем зарегистрированным событиям риска ИБ, с ненулевой величиной прямых потерь, о которых кредитная организация сообщила в своих отчетах в ФинЦЕРТ.

2.1.2. Кредитные организации, применяющие продвинутый подход к расчету необходимого капитала на покрытие операционного риска, кроме базовых показателей системы управления риском ИБ, перечисленных в пункте 2.1.1 настоящего Приложения, используют следующие дополнительные показатели:

прямые и косвенные потери, определяемые расчетным образом, от реализации событий риска ИБ за определенный период (наращенным итогом за 3, 6, 9 месяцев и год);

отношение прямых и косвенных потерь, определяемых расчетным образом, от событий риска ИБ, понесенных кредитной организации за годовой

период к собственным средствам (капиталу) кредитной организации на последнюю отчетную дату года;

отношение сумм прямых и косвенных потерь, определяемых расчетным образом, кредитной организации за определенный период (наращенным итогом за 3, 6, 9 месяцев и год) при выполнении кредитной организацией функций оператора иных платежных систем или оператора услуг платежной инфраструктуры к общей сумме операций по переводу денежных средств через иных платежных системы или платежной инфраструктуры за этот же период;

прямые и косвенные потери, определяемые расчетным образом, кредитной организации в результате использования электронных средств платежа клиентов кредитных организаций без их согласия;

прямые и косвенные потери, определяемые расчетным образом, кредитной организации в результате переводов и снятий денежных средств, связанных с несанкционированным доступом к объектам информационной инфраструктуры кредитной организации;

2.2. К качественным показателям системы управления рисками ИБ относятся, качественные оценки по четырехуровневой системе (хорошо, удовлетворительно, сомнительно, неудовлетворительно):

оценка качества функционирования системы управления риском ИБ, проведенная уполномоченным подразделением либо внешним экспертом - специализированной организацией или квалифицированным внешним экспертом, проведенной по решению совета директоров (наблюдательного совета) кредитной организации;

для кредитных организаций – участников платежной системы Банка России – оценка соблюдения кредитной организацией требований нормативных актов Банка России, разработанных в соответствии со статьей 20 и пунктом 3 статьи 27 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе», Положением Банка России № 382-П, Положением Банка России № 552-П;

для кредитных организаций – оценка соответствия системы мер в области обеспечения информационной безопасности по направлениям деятельности, в соответствии с пунктом 2.10 настоящего Положения, положениям национальных стандартов Российской Федерации, в том числе стандарта ГОСТ Р 5780.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия» и нормативных актов Банком России.

Приложение 5
к Положению Банка России
от «___»_____ 201__ № _____-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Подходы к расчету капитала, необходимого на покрытие потерь от реализации операционного риска.

1. Кредитная организация (головная кредитная организация банковской группы) в зависимости от характера и масштаба деятельности в целях применения абзаца 3 пункта 4.9.1 Указания Банка России № 3624-У выбирает один из следующих подходов к расчету капитала, необходимого для покрытия потерь от операционного риска (далее – необходимый капитал) в рамках внутренних процедур оценки достаточности капитала (далее – ВПОДК) в соответствии с Указанием Банка России № 3624-У:

регуляторный подход на базе расчета минимального регуляторного капитала на покрытие операционного риска на основе Положения Банка России № 346-П и прогнозных сценариев среднегодовых потерь от реализации событий операционного риска и событий риска ИБ, изложенный в пункте 4 настоящего Приложения;

продвинутый подход на базе внутренних моделей количественной оценки потерь от реализации операционного риска на основе статистики базы данных о событиях операционного риска и событий риска ИБ (с использованием статистики за период не менее 5 лет) с использованием методов, применяемых в международной практике.

2. В случае, когда необходимый капитал на покрытие потерь от реализации операционного риска для целей ВПОДК по продвинутому подходу оказывается меньше, чем минимальный регуляторный капитал на покрытие операционного риска, определяемый в соответствии с пунктом 3 настоящего

Приложения, исполнительный орган кредитной организации в составе материалов на совет директоров по утверждению стратегии управления рисками и капиталом представляет мотивированное суждение, содержащее обоснование, что уровень операционного риска в кредитной организации оценивается им ниже, чем требуется в соответствии с регуляторным подходом и направляет данное мотивированное суждение в составе материалов, предоставляемых в Банк России в ходе надзорной оценки системы управления операционным риском в соответствии с главой 9 настоящего Положения.

3. Кредитная организация (головная кредитная организация банковской группы), выбравшая в соответствии с пунктом 1 настоящего Приложения регуляторный подход, определяет объем необходимого капитала на покрытие операционного риска для целей ВПОДК как сумму трех компонент:

$$К_{\text{необ\_К}i,\text{ОР}} = К_{\text{мин\_ К}i,\text{ОР}} + \Delta_{Ki,\text{ИБ}} + \Delta_{Ki,\text{ОР}}$$

где:

$К_{\text{необ\_Кi,ОР}}$ – необходимый капитал для целей ВПОДК на покрытие потерь от реализации событий операционного риска, включаемый в состав капитала Кi, определенный в соответствии с методикой, предусмотренной Положением Банка России от 28 декабря 2012 года № 395-П «Положение о методике определения величины собственных средств (капитала) кредитных организаций («Базель III»)», зарегистрированным Министерством юстиции Российской Федерации 22 февраля 2013 года № 27259 («Вестник Банка России» от 27 февраля 2013 года № 11);

$К_{\text{мин\_Кi,ОР}}$ – минимальный регуляторный капитал, включаемый в состав капитала Кi и выделяемый на покрытие потерь от реализации событий операционного риска, необходимый для соблюдения минимально допустимого числового значения соответствующего норматива достаточности капитала Н1.i, определённого в пункте 2.1.1 Инструкции Банка России от 28.06.2017 N 180-И «Об обязательных нормативах банков» (далее –

Инструкция Банка России № 180-И):

$$К_{мин\_Ki,ОР} = 12{,}5 * ОР * Н1.i_{мин}$$

где:

Н1.i,мин – минимально допустимое числовое значение норматива соответствующего норматива достаточности капитала Н1.i, определённое в пункте 2.2 Инструкции Банка России № 180-И;

ОР – целевое (прогнозное) значение на планируемый период размера операционного риска, определяемого в соответствии с Положением Банка России № 346-П;

$Δ_{Ki,ИБ}$ – компонента необходимого капитала для целей ВПОДК в составе капиталов К1, К2, К0 соответственно на покрытие прямых потерь для $Δ_{К1,ИБ}$ и $Δ_{К2,ИБ}$ прямых потерь (для $Δ_{К0,ИБ}$ – совокупных (прямых и косвенных) потерь) от реализации событий риска ИБ, которые определяются кредитной организацией на базе сценарного моделирования (стресс-тестирования) в части возможного превышения фактической величины прямых (совокупных) потерь над контрольным (лимитным значением) соответствующего контрольного показателя уровня операционного риска – лимита прямых (совокупных) годовых потерь от реализации событий риска ИБ), установленного в соответствии с пунктом 2.1.1 Приложения 4 к настоящему Положению;

$Δ_{Ki,ОР}$ – компонента необходимого капитала для целей ВПОДК в составе капиталов К1, К2, К0 соответственно на покрытие для $Δ_{К1,ОР}$ и $Δ_{К2,ОР}$ прямых потерь (для $Δ_{К0,ОР}$ – совокупных (прямых и косвенных) потерь) от реализации операционного риска за вычетом потерь от событий риска ИБ, которые определяются кредитной организацией на базе сценарного моделирования (стресс-тестирования) в части возможного превышения фактической величины прямых (совокупных) потерь над контрольным (лимитным

значением) соответствующего контрольного показателя уровня операционного риска – лимита прямых (совокупных) годовых потерь от реализации событий операционного риска за вычетом лимита прямых потерь от реализации событий риска ИБ, установленного в соответствии с пунктом 1.1.1 Приложения 4 к настоящему Положению.

4. Если кредитная организация применяет регуляторный подход к оценке необходимого капитала для целей ВПОДК и фактическая совокупная величина прямых годовых потерь от реализации событий операционного риска и событий риска ИБ за каждый год не превышала минимальный регуляторный капитал соответствующего года на протяжении последних 10 лет, то кредитная организация может соответствующую компоненту необходимого капитала на покрытие потерь от реализации событий риска ИБ и (или) событий операционного риска приравнять к нулю на базе мотивированного суждения службы управления рисками об отсутствии иных факторов возможных потерь, например, отсутствии существенных изменений внутренних и внешних факторов операционной среды кредитной организации с приложением результатов сценарного моделирования и стресс-тестирования.

4.1. Если у кредитной организации нет данных о потерях от реализации событий операционного риска и событий риска ИБ за 10 лет, то кредитная организация может использовать в целях расчета необходимого капитала для целей ВПОДК накопленные данные за имеющейся период, но не менее 3 лет, с учетом включения накопленных данных о потерях последующих лет до достижения периода в 10 лет, для сравнения с минимальным регуляторным капиталом соответствующего года.

При этом, кредитная организация (головная кредитная организация банковской группы) ежегодно готовит мотивированное суждение при формировании необходимого капитала для целей ВПОДК о достаточности

имеющихся накопленных данных о потерях от реализации событий операционного риска и (или) событий риска ИБ для установления нулевых значений компонент необходимого капитала на покрытие потерь от реализации событий операционного риска и (или) событий риска ИБ.

4.2. Если у кредитной организации нет данных о потерях от реализации событий операционного риска и (или) событий риска ИБ за 3 года или накопленные данные не соответствуют требованиям главы 6 настоящего Положения, то кредитная организация не может установить нулевые значения компонент $\Delta_{\text{К}i,\text{ИБ}}$ и $\Delta_{\text{К}i,\text{ОР}}$ и, при определении объема необходимого капитала на покрытие операционного риска для целей ВПОДК, кредитная организация должна определять значение данных компонент с учетом сценарного моделирования.

4.3. Служба управления рисками подготавливает мотивированное суждение об отсутствии иных факторов возможных потерь и направляет его на рассмотрение исполнительному органу кредитной организации.

4.4. Исполнительный орган кредитной организации рассматривает мотивированное суждение об отсутствии иных факторов возможных потерь и утверждает его в рамках планирования капитала в соответствии с третьим абзацем пункта 1.2 Указания Банка России № 3624-У.

5. Кредитная организация (головная кредитная организация банковской группы), выбравшая в соответствии с пунктом 1 настоящего Приложения продвинутый подход на базе внутренних моделей, определяет объем необходимого капитала для целей ВПОДК в составе капитала Кi на покрытие потерь от реализации операционного риска в соответствии с методикой количественной оценки прямых потерь (для необходимого капитала в составе базового и основного капиталов) и совокупных потерь (для необходимого капитала в составе собственных средств) от реализации операционного риска (далее – методика потерь), с заданным во внутренних документах

доверительной вероятностью как сумму двух компонент:

необходимого капитала на покрытие потерь от реализации событий риска ИБ;

необходимого капитала на покрытие потерь от реализации операционного риска за вычетом риска ИБ.

При этом для оценки необходимого капитала для целей ВПОДК в дополнение к потерям от реализации внутренних событий операционного риска кредитная организация должна использовать информацию о потерях из внешних баз данных о событиях операционного риска, с использованием методов сценарного моделирования, в соответствии с пунктом 4.3 главы 4 Приложения 1 Указания Банка России № 3624-У.

6. Если фактическая величина потерь от реализации событий операционного риска и (или) событий риска ИБ по итогам года превысила выделенную на этот год величину необходимого капитала на покрытие соответствующих потерь для целей ВПОДК, то данное превышение добавляется в течение последующего года к оценке соответствующей компоненты необходимого капитала, рассчитанной по потерям из базы событий.

7. Кредитная организация (головная кредитная организация банковской группы), учитывающая потери от реализации операционного риска и (или) риска ИБ в запланированных расходах кредитной организации соответствующего года, при определении сигнального (приемлемого) уровня прямых или совокупных потерь, может уменьшать соответствующие компоненты необходимого капитала на величину, не превышающую величину запланированных расходов от реализации операционного риска и (или) риска ИБ.

8. Кредитная организация (головная кредитная организация банковской

группы), применяющая отдельные механизмы и процедуры управления отдельными видами операционного риска, вправе в составе необходимого капитала на покрытие операционного риска для целей ВПОДК выделять дополнительные компоненты необходимого капитала на покрытие этих видов операционного риска.