ПРОЕКТ

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЛОЖЕНИЕ

от __ _____2019 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; 2017, № 1, ст. 46; № 14, ст. 1997; № 18, ст. 2661, 2669; № 27, ст. 3950; № 30, ст. 4456; № 31, ст. 4830; 2018, № 11, ст. 1584, 1588; № 18, ст. 2557; № 24 ст. 3400; № 27, ст. 3950; №31 ст. 4852; № 32 ст. 5115; № 49 ст. 7524; № 53 ст. 8411, 8440) (далее – Федеральный закон

№ 86-ФЗ) Банк России устанавливает требования к системе управления операционным риском в кредитной организации и банковской группе, за исключением центрального контрагента, в значении, установленном в статье 2 Федерального закона от 7 февраля 2011 года № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте» (Собрание законодательства Российской Федерации, 2011, № 7, ст. 904; № 48, ст. 6728; № 49 ст. 7040, 7061; 2012, № 53, ст. 7607; 2013, № 30, ст. 4084; 2014, № 11, ст. 1098; 2015, № 27, ст. 4001; № 29, ст. 4357; 2016, № 1, ст. 23, 47; 2017, № 30, ст. 4456; 2018, № 24, ст. 3399; № 31, ст. 4861; № 53, ст. 8440), включая требования к ведению аналитической базы данных о событиях операционного риска и потерях, понесенных вследствие его реализации, в соответствии с пунктом 4.3 приложения 1 к Указанию Банка России от 15 апреля 2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы», зарегистрированному Министерством юстиции Российской Федерации 26 мая 2015 года № 37388, 28 декабря 2015 года № 40325, 7 декабря 2017 года № 49156, 5 сентября 2018 года № 52084 (далее – Указание Банка России № 3624-У).

Глава 1. **Общие положения**

1.1. Настоящее Положение устанавливает требования к системе управления операционным риском кредитной организации (головной кредитной организации банковской группы).

Операционный риск определяется в значении, указанном в пункте 4.1 приложения 1 к Указанию Банка России № 3624-У.

Кредитная организация (головная кредитная организация банковской группы) организует систему управления операционным риском с соблюдением требований настоящего Положения и Указания Банка России № 3624-У.

1.2. Кредитная организация (головная кредитная организация банковской группы) выявляет случаи фактической реализации операционного риска (далее – событие операционного риска) в соответствии с главой 3

настоящего Положения, классифицирует события операционного риска в соответствии с главой 2 настоящего Положения и фиксирует события операционного риска в аналитической базе данных о событиях операционного риска и потерях, понесенных вследствие его реализации, (далее – база событий) в соответствии с главой 6 настоящего Положения.

1.3. Система управления операционным риском в кредитной организации состоит из следующих элементов:

процедур управления операционным риском в соответствии с пунктом 4.1 приложения 1 к Указанию Банка России № 3624-У и требованиями главы 3 настоящего Положения;

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

базы событий, содержащей информацию о событиях операционного риска и потерях от всех видов операционного риска;

контрольных показателей кредитной организации в соответствии с главой 5 настоящего Положения;

системы мер, направленной на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска, установленного кредитной организацией в соответствии с подпунктом 4.1.5 пункта 4.1 настоящего Положения;

подразделения кредитной организации (подразделений участников банковской группы) по организации управления операционным риском, структурно входящего в службу управления рисками кредитной организации (службу управления рисками участника банковской группы) (далее – подразделение, ответственное за организацию управления операционным риском);

специализированных подразделений кредитной организации (специализированных подразделений участников банковской группы), которые выполняют процедуры управления операционным риском, указанные в пунктах 3.3, 3.7 и 3.9 настоящего Положения в части отдельных видов

операционного риска, определенных в пункте 1.4 настоящего Положения. В случае если указанные специализированные подразделения организационно независимы от службы управления рисками кредитной организации (головной кредитной организации банковской группы), функции управления отдельными видами операционного риска исполняются работниками специализированных подразделений, координация деятельности таких работников, связанная с управлением операционным риском, в части соблюдения процедур управления операционным риском, обмена информации, предоставления отчетности и других элементов взаимодействия, в соответствии с порядком, установленным в документах кредитной организации, осуществляется руководителем подразделения, ответственного за организацию управления операционным риском;

подразделений-владельцев банковских процессов кредитной организации (подразделений-владельцев банковских процессов участников банковской группы) и подразделений, обеспечивающих банковские процессы кредитной организации (далее – центров компетенций), осуществляющих выявление операционного риска, сбор информации и информирование о выявленном операционном риске как подразделения, ответственного за организацию управления операционным риском, так и подразделения - владельца процесса, в котором выявлен операционный риск (в случае если операционный риск выявлен в деятельности другого подразделения кредитной организации), оценку выявленных операционных рисков, присущих процессам центров компетенций (в пределах своей компетенции), разработку и внедрение мер, направленных на уменьшение негативного влияния операционного риска, а также мониторинг уровня операционного риска в своих процессах;

автоматизированной информационной системы, объем и функциональность которой определяется характером и масштабом осуществляемых операций и действующих банковских процессов кредитной организации (головной кредитной организации банковской группы),

обеспечивающей функционирование как в целом системы управления операционным риском, так и отдельных ее элементов, в том числе базы событий, с обеспечением сохранности и защиты данных от искажений информации;

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

1.4. Кредитная организация (головная кредитная организация банковской группы) для целей унификации управления операционным риском выделяет следующие виды операционного риска, процедуры по которым выполняются в соответствии с абзацем 8 пункта 1.3 настоящего Положения специализированными подразделениями кредитной организации (специализированными подразделениями участников банковской группы), к которым предъявляются общие требования в рамках системы управления операционным риском в соответствии с настоящим Положением:

риск информационной безопасности (далее – риск ИБ), определяемый в соответствии с пунктом 7.1 настоящего Положения;

риск информационных систем (далее – риск ИС), определяемый в соответствии с пунктом 8.1 настоящего Положения;

правовой риск, определяемый в соответствии с пунктом 3.3 Указания Банка России № 3624-У;

риск ошибок в управлении проектами (далее – проектный риск по причине операционного риска);

риск ошибок и недостатков управленческих процессов (далее – управленческий риск по причине операционного риска);

риск нарушения процедур контроля, в том числе нарушения правил противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;

модельный риск, определяемый в значении, установленном в пункте 4.2 приложения 1 к Указанию Банка России № 3624-У, связанный с реализацией операционного риска;

риск потерь клиентов, контрагентов и третьих лиц вследствие нарушения кредитной организацией норм взаимодействия с клиентами и рыночных практик (далее – риск поведения);

риск ошибок и недостатков процесса управления персоналом (далее - риск персонала);

другие виды операционного риска.

1.5. Единоличный и коллегиальный исполнительные органы кредитной организации (головной кредитной организации банковской группы) в соответствии с пунктом 2.4 Указания Банка России № 3624-У утверждают документы, регламентирующие процедуры управления операционным риском в кредитной организации (участнике банковской группы), в том числе документы, предусмотренные настоящим Положением, а также обеспечивают их исполнение в соответствии с требованиями настоящего Положения.

Глава 2. **Элементы классификации событий операционного риска, используемые в системе управления операционным риском**

2.1. Кредитная организация (головная кредитная организация банковской группы) классифицирует все события операционного риска в разрезе следующих элементов: источников риска, типов событий, направлений деятельности, в том числе в разрезе составляющих их банковских процессов, и видов потерь.

2.2. Кредитная организация (головная кредитная организация банковской группы) для всех видов операционного риска определяет в документах единый классификатор источников риска, направлений деятельности, типов событий, видов потерь от реализации операционного риска. Единый классификатор должен обновляться с учетом изменений характера и масштаба деятельности.

В целях контроля со стороны Банка России состояния базы событий кредитная организация (головная кредитная организация банковской группы) устанавливает процедуру ежемесячного (на отчетную дату) соотнесения внутренней классификации событий операционного риска кредитной организации с классификацией, предусмотренной требованиями главы 2 настоящего Положения.

2.3. Источники операционного риска классифицируются на следующие категории.

2.3.1. К первой категории относятся ошибки и недостатки процессов, в том числе ненадежная и (или) неэффективная организация внутренних процессов управления в кредитной организации и проведения банковских и других операций (далее – процессы), а также несоответствие указанных процессов 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 других связанных с кредитной организацией лиц, включая собственников, а также лиц, связанных с кредитной организацией в рамках договорных отношений по выполнению работ (оказанию услуг) (далее – действия персонала);

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

2.3.4. К четвертой категории относятся воздействия внешних причин, включая действия третьих лиц, в том числе действия государственных и регулирующих органов, правоохранительных органов, других организаций, а также другие воздействия внешнего характера (далее – внешние факторы).

2.4. Кредитная организация (головная кредитная организация банковской группы) классифицирует все события операционного риска в разрезе источников операционного риска.

В случае если в событии операционного риска выявляется несколько источников операционного риска, кредитная организация (головная кредитная организация банковской группы) указывает в базе событий все выявленные источники события операционного риска.

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

2.6. У одного и того же события операционного риска должен быть один или более источник операционного риска. В этом случае в отношении реализовавшегося события операционного риска в базе событий кредитная организация указывает все выявленные источники событий операционного риска и экспертным образом определяет наиболее значимый источник риска. Кредитная организация определяет в документах правила определения наиболее значимого источника риска.

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

2.7.1. Проведение преднамеренных действий с участием как минимум одного работника кредитной организации, направленных на присвоение (хищение), уничтожение (нанесение ущерба) материальных и нематериальных активов или другого имущества кредитной организации и (или) средств клиентов, ухудшение работы банковских процессов, недостижение целей

кредитной организации, в том числе случаи умышленного несоблюдения нормативных актов или документов кредитной организации в целях извлечения материальной и нематериальной выгоды (далее – неразрешенные действия персонала).

2.7.2. Проведение преднамеренных действий, совершаемых третьими лицами, направленных на присвоение (хищение), уничтожение (нанесение ущерба) материальных и нематериальных активов или другого имущества кредитной организации и (или) средств клиентов, ухудшение работы банковских процессов и систем, недостижение целей кредитной организации, приобретение прав на имущество кредитной организации обманным путем или в нарушение действующего законодательства (далее – преднамеренные действия третьих лиц).

2.7.3. Нарушения кадровой политики и безопасности труда со стороны кредитной организации, включая нарушения трудового законодательства, требований по охране труда, охране здоровья или связанные с выплатами работникам кредитной организации по требованиям (в том числе 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 нарушения кодексов поведения на рынках, 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, вандализма и военных действий.

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

2.7.7. Нарушения организации, исполнения и управления процессами кредитной организации, включая ошибки при обработке операций, недостатки обеспечения функционирования банковских процессов, недостатки систем управления рисками, внутреннего контроля, учета и отчетности, системы обеспечения информационной безопасности, процедур противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения, недостатки в процессах взаимоотношений с торговыми контрагентами и поставщиками, за исключением действий, перечисленных в подпункте 2.7.1 настоящего пункта Положения.

2.8. Для отдельных видов операционного риска, для целей классификации событий операционного риска в базе событий, применяются 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) определяет в документах классификацию типов событий операционного риска до второго уровня и более с учетом характера и масштаба деятельности кредитной организации (головной кредитной организации банковской группы). Классификация типов событий операционного риска второго уровня представлена в приложении 1 к настоящему Положению.

2.10. События операционного риска классифицируются по основным направлениям деятельности (в разрезе составляющих их банковских процессов) кредитной организации следующим образом (далее – классификация направлений деятельности первого уровня):

2.10.1. корпоративное финансирование – оказание услуг юридическим лицам, 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;

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

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

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

2.10.5. осуществление переводов денежных средств, 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 банковским процессам других направлений деятельности;

2.10.6. 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;

2.10.7. управление активами – управление активами клиентов по договорам доверительного управления;

2.10.8. розничное брокерское обслуживание – брокерское обслуживание розничных клиентов;

2.10.9. обеспечение деятельности кредитной организации – обеспечивающие и организационные направления деятельности (например, бухгалтерский учет, административно-хозяйственная деятельность, управление рисками, деятельность по обеспечению функционирования информационных систем, обеспечение физической безопасности,

противопожарной безопасности и охраны труда, юридическое сопровождение, управление персоналом и другие).

Кредитная организация (головная кредитная организация банковской группы) расширяет классификацию направлений деятельности (в разрезе составляющих их банковских процессов) до второго уровня и более с учетом характера и масштаба деятельности кредитной организации.

2.11. Потери в результате реализации события операционного риска делятся на прямые и непрямые потери кредитной организации, а также потери (включая хищения) денежных средств клиентов и третьих лиц, которые не были компенсированы кредитной организацией.

2.11.1. Прямые потери кредитной организации (участника банковской группы), 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», зарегистрированным Министерством юстиции Российской Федерации 6 февраля 2015 года № 35910, 8 декабря 2015 года № 40025, 12 декабря 2017 года № 49219, 31 июля 2018 года № 51743, и приравненных к ним счетах по учету дебиторской задолженности, классифицируются по следующим видам.

2.11.1.1. Снижение (обесценение) стоимости активов. Данный вид потерь включает в себя следующие виды потерь второго уровня:

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;

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

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

потери, отраженные на других счетах бухгалтерского учета, отнесенные к счетам расходов;

расходы, связанные с возвратом кредитных средств и других финансовых активов, возникших по причине операционного риска;

отрицательная переоценка стоимости торгового портфеля и (или) финансового инструмента из-за нарушения правил совершения сделок и операций с инструментами торгового портфеля, в том числе из-за нарушения правил совершения банковских операций, определенных в документах кредитной организации (например, нарушение лимита сделки);

начисление амортизационных расходов по причине операционного риска (например, при списании с баланса оборудования, украденного, испорченного или уничтоженного в результате события операционного риска).

2.11.1.2. Досрочное списание (выбытие, потеря, уничтожение) материальных и нематериальных, финансовых активов в результате реализации события операционного риска.

2.11.1.3. Денежные выплаты клиентам и контрагентам в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине кредитной организации, в том числе компенсированные кредитной организацией хищения средств клиентов и третьих лиц (с раздельным учетом потерь, которые были компенсированы кредитной организацией в составе прямых потерь, которые были компенсированы сторонними третьими лицами (например, страховыми компаниями).

2.11.1.4. Денежные выплаты работникам кредитной организации в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине кредитной организации.

2.11.1.5. Потери от ошибочных платежей, включающие:

потери в размере ошибочного платежа;

потери в виде уплаченных комиссий по проведению ошибочного платежа;

потери, связанные с поиском возможности возврата ошибочного платежа.

2.11.1.6. Судебные издержки, включающие:

расходы на работников кредитной организации, представляющих интересы кредитной организации в суде, по делам, связанным с реализацией событий операционного риска;

выплаты и компенсации по решению суда, по делам, связанным с реализацией событий операционного риска;

расходы на адвокатов и судебных представителей, по делам, связанным с реализацией событий операционного риска;

начисление резервов некредитного характера по предъявленным претензиям и судебным искам.

2.11.1.7. Штрафы и санкции, наложенные надзорными или административными органами.

2.11.1.8. Расходы на устранение последствий реализации события операционного риска, направленные на восстановление деятельности или на снижение потерь от реализовавшегося события операционного риска.

2.11.1.9. Экономический убыток от невыгодных для кредитной организации сделок по причине операционного риска.

2.11.1.10. Прочие расходы, связанные с реализацией событий операционного риска или устранением последствий события операционного риска.

2.11.2. Непрямые потери кредитной организации (участника банковской группы), 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 (далее – качественные потери), в случае если потери не выражены в денежном

выражении расчетным способом в соответствии с подпунктом 2.11.2.1 настоящего пункта Положения.

2.11.2.1. Косвенные потери включают в себя:

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

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

расходы на реализацию системы мер, направленной на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска в соответствии с подпунктом 4.1.5 пункта 4.1 настоящего Положения, связанные с устранением причин реализации событий операционного риска, направленные на улучшение банковских процессов, не отнесенные к прямым потерям от реализации событий операционного риска;

потери кредитной организации, не реализовавшиеся в виде прямых и косвенных потерь, но которые возникли бы при реализации не выявленных источников риска и (или) неблагоприятного стечения обстоятельств, 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 или инструментов капитала кредитной организации, в том числе стоимости привлечения субординированных кредитов, как источника капитала второго уровня, из-за события операционного риска;

расходы, связанные с восстановлением ликвидности из-за оттока денежных средств по причине реализации 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, рыночного риска, риска ликвидности, риска потери деловой репутации, регуляторного риска, стратегического риска);

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

отток клиентов;

срыв сделки и (или) неоказание банковской услуги;

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 процессов и операций);

утечку, потерю или искажение защищаемой, в том числе коммерческой, информации;

предписания надзорных, правоохранительных органов, не связанные с финансовыми санкциями и уплатой штрафов;

снижение лимитов на межбанковское кредитование;

другие качественные потери.

Кредитная организация проводит оценку значимости качественных потерь в соответствии с принятой в кредитной организации шкалой качественных оценок (например, по четырехуровневой шкале: «очень высокие», «высокие», «средние», «низкие»).

Кредитная организация устанавливает критерии шкалы и методику качественных оценок для определения качественных потерь от события операционного риска.

2.11.3. Потери (в том числе хищения) средств клиентов и третьих лиц, которые не были компенсированы кредитной организацией:

потери средств физических лиц и индивидуальных предпринимателей;

потери средств юридических лиц;

потери средств третьих лиц;

штрафы, наложенные на должностных лиц кредитной организации за осуществление (неосуществление) профессиональной деятельности;

другие потери (в том числе хищения).

2.12. Кредитная организация (головная кредитная организация банковской группы) в документах определяет дополнительные классификации видов потерь, включая порядок их определения и актуализации.

Глава 3. **Требования к процедурам управления операционным риском**

3.1. Кредитная организация (головная кредитная организация банковской группы) устанавливает в документах процедуры управления операционным риском в соответствии с требованиями настоящей главы и в соответствии с пунктом 4.1 приложения 1 к Указанию Банка России № 3624-У.

3.2. Процедура выявления и идентификации операционного риска включает следующие способы:

3.2.1. анализ базы событий в соответствии с пунктом 3.3 настоящего Положения;

3.2.2. проведение ежегодной самооценки операционного риска и форм (способов) контроля, направленных на его снижение (качественной экспертной оценки уровня операционных рисков) на основе формализованных анкет, в соответствии с требованиями подпункта 3.6.5 пункта 3.6 настоящего Положения;

3.2.3. анализ динамики ключевых индикаторов риска по направлениям деятельности в разрезе составляющих их банковских процессов кредитной организации в соответствии с подпунктом 3.9.2 пункта 3.9 настоящего Положения;

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

3.2.5. анализ актов проверок, предписаний Банка России, правоохранительных органов или других надзорных органов, в части фактов, относящихся к реализации операционного риска;

3.2.6. анализ информации внутреннего и внешнего аудита кредитной организации;

3.2.7. анализ информации работников кредитной организации, полученной в рамках инициативного информирования работниками кредитной организации службы управления рисками и (или) службы внутреннего аудита;

3.2.8. анализ других внешних и внутренних источников информации и способов выявления рисков.

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:

3.3.1. автоматизированное выявление информации из информационных систем о реализовавшихся или возможных к реализации событиях операционного риска;

3.3.2. выявление и сбор информации о событиях операционного риска в ручном режиме, предусматривающий экспертное выявление информации и проведение анализа обстоятельств и причин произошедших событий операционного риска, в случае если автоматизированное выявление и сбор информации о событиях операционного риска невозможно. Порядок и срок

проведения анализа обстоятельств и причин произошедших событий операционного риска определяется в документах кредитной организации;

3.3.3. ввод информации о событиях операционного риска в базу событий по алгоритмизированным правилам, установленным кредитной организацией в документах;

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

3.3.5. определение потерь от событий операционного риска в соответствии с пунктом 3.4 настоящего Положения;

3.3.6. регистрацию событий операционного риска в базе событий;

3.3.7. определение и оценка стоимости полученных возмещений в базе событий;

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

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

3.3.10. Кредитная организация (головная кредитная организация банковской группы) обеспечивает соблюдение процедуры сбора и регистрации информации о внутренних событиях операционного риска и потерях по всем направлениям деятельности в разрезе составляющих их банковских процессов с указанием в документах:

владельцев процессов и центров компетенций, ответственных за выявление и сбор информации о событиях и выполнения других процедур управления операционным риском;

правил предоставления информации центрами компетенций в подразделение, ответственное за организацию управления операционным риском, не позднее пяти рабочих дней с момента идентификации события операционного риска;

показателей, указанных в абзацах 2 и 6 подпункта 1.1.1 пункта 1 и абзацах 2 и 9 подпункта 2.1.1 пункта 2 приложения 4 к настоящему Положению в разрезе центров компетенций (ключевых показателей эффективности по выявлению событий операционного риска в банковских процессах), несоблюдение которых предусматривает ответственность центров компетенций (их руководителей).

3.4. Процедура определения потерь и возмещений от событий операционного риска включает:

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

3.4.2. методы и порядок определения непрямых потерь кредитной организации от события операционного риска в базе событий;

3.4.3. методы и порядок определения потерь клиентов и третьих лиц (не компенсированных кредитной организацией) от события операционного риска в базе событий;

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

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

3.4.6. порядок и методы определения потенциальных потерь (для определения непрямых потерь);

3.4.7. порядок и методы определения и оценки стоимости возмещений от событий операционного риска;

3.4.8. отбор и назначение экспертов кредитной организации, ответственных за расчет потерь от событий операционного риска в разрезе направлений деятельности и банковских процессов, областей их компетенции и ответственности. Допускается совмещение функции регистрации событий

операционного риска в базе событий, расчета потерь и возмещений от событий операционного риска.

3.5. Процедура количественной оценки уровня операционного риска, включает:

3.5.1. агрегированную оценку уровня операционного риска по кредитной организации в целом, по подразделениям кредитной организации, а также по направлениям деятельности в разрезе составляющих их банковских процессов, в соответствии с пунктом 2.10 настоящего Положения и видов операционного риска, в соответствии с пунктом 1.4 настоящего Положения;

3.5.2. оценку необходимого капитала для целей ВПОДК на покрытие потерь от событий операционного риска в целом по кредитной организации и в разрезе направлений деятельности и видов операционного риска (например, по риску ИБ) с учетом подходов, изложенных в приложении 5 к настоящему Положению;

3.5.3. оценку ожидаемых потерь от реализации операционного риска в разрезе направлений деятельности и банковских процессов, по которым наблюдается соответствующая статистика событий операционного риска, в целях покрытия этих потерь в ценообразовании соответствующих банковских услуг и тарифов (при наличии). Кредитная организация устанавливает в документах методы и порядок проведения оценки ожидаемых потерь от реализации операционного риска.

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

3.6.1. самооценку операционного риска и форм (способов) контроля, направленных на снижение его уровня (далее – самооценка операционного риска), в соответствии с подпунктом 3.6.5 настоящего пункта Положения;

3.6.2. экспертную профессиональную оценку (профессиональное мнение внутренних и внешних экспертов) с учетом установленных кредитной

организацией в документах правил и порядка определения правил привлечения внешних экспертов,

3.6.3. автоматизированную оценку с использованием программного обеспечения;

3.6.4. сценарный анализ операционных рисков.

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

Подразделение, ответственное за организацию управления операционным риском, разрабатывает на ежегодной основе план проведения качественной оценки уровня операционного риска, который утверждается коллегиальным исполнительным органом кредитной организации и включает определение ответственных и участвующих подразделений кредитной организации.

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

3.6.5. Самооценка операционного риска проводится кредитной организацией (головной кредитной организацией банковской группы) не реже одного раза в год по установленной в 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.

Кредитная организация определяет критерии самооценки операционного риска, которые должны включать:

критерии оценки уровня существенности операционного риска (с возможностью соотнесения к 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 негативного влияния оцениваемого риска), действующих на момент проведения оценки;

критерии оценки уровня возможных потерь при реализации операционного риска с учетом оценки эффективности форм (способов) контролей (далее - уровень остаточного риска).

3.6.6. Кредитная организация (головная кредитная организация банковской группы) разрабатывает требования к проведению экспертной профессиональной оценки уровня операционного риска внутренними и внешними экспертами с указанием сроков, правил и порядка ее проведения.

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

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

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

3.7. 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);

передачу риска (страхование, передача риска другой стороне - контрагенту и (или) клиенту);

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

принятие мер, направленных на уменьшение негативного влияния операционного риска на качество процессов, величину совокупных (валовых) потерь (разработка кредитной организацией форм (способов) контроля и мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска), которые включают:

реинжиниринг банковских процессов;

установление дополнительных форм (способов) контроля;

обучение работников, в том числе участников банковских процессов;

применение автоматизированных решений;

другие меры, направленные на уменьшение негативного влияния операционного риска.

Рекомендуемый перечень возможных мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска, приведен в приложении 3 к настоящему Положению.

Кредитная организация определяет в документах способы реагирования на операционный риск в зависимости от уровня потерь от операционного риска, реализации событий операционного риска.

3.8. Кредитная организация (головная кредитная организация банковской группы) определяет порядок выбора способа реагирования, в соответствии с пунктом 3.7 настоящего Положения, в том числе и методы оценки стоимости выбранного способа реагирования.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает меры, направленные на снижение негативного влияния

операционного риска с учетом оценки эффективности и уровня остаточного риска (по результатам реализации мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска).

3.9. Процедура мониторинга операционного риска включает:

установление и мониторинг ключевых индикаторов 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 повышение качества системы управления операционным риском и 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, единоличного и коллегиального органов управления кредитной организации, других источников информации.

Кредитная организация определяет в документах состав процедур мониторинга операционного риска.

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

3.9.2. Кредитная организация (головная кредитная организация банковской группы) в документах устанавливает требования к КИР и к их документированию, включающие:

количественное измерение КИР;

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

периодичность (не реже одного раза в квартал) проведения оценки в целях пересмотра КИР для обеспечения поддержания КИР в актуальном состоянии;

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

процедуры валидации значений и данных КИР для проверки корректности расчета;

состав информации, используемой для расчета КИР и их источников, включая способ получения информации;

пороговые значения КИР;

наименование операционного риска (несколько операционных рисков), которых отслеживает КИР;

ответственное подразделение кредитной организации, отвечающее за предоставление данных для расчета КИР и (или) расчет КИР;

порядок реагирования на превышение пороговых значений КИР.

3.9.3. Кредитная организация (головная кредитная организация банковской группы) направляет результаты процедуры мониторинга операционного риска на рассмотрение коллегиальному исполнительному органу кредитной организации (другим коллегиальным исполнительным органам, например, комитетом по управлению операционным риском) в составе ежеквартального и годового отчета об управлении операционным риском, в соответствии с абзацем 2 подпункта 4.2.1.2, подпунктом 4.2.1.3 пункта 4.2 настоящего Положения.

3.10. Кредитная организация (головная кредитная организация банковской группы) предусматривает в документах, регламентирующих процедуры управления операционным риском, роли и ответственность подразделений кредитной организации, закрепление ответственности за

выявление операционного риска, сбор информации о событиях операционного риска и потерях, участие в качественной оценке операционного риска в части их функций и компетенции за подразделениями-владельцами процессов и подразделениями-участниками процессов, в значении, установленном в подпункте 4.1.1 пункта 4.1 настоящего Положения.

3.11. Кредитная организация (головная кредитная организация банковской группы) включает информацию о результатах проведения процедур управления операционным риском, установленных пунктами 3.2-3.9 настоящего Положения, в состав ежеквартального и годового отчета об управлении операционным риском, в соответствии с абзацем 2 подпункта 4.2.1.2, подпунктом 4.2.1.3 пункта 4.2 настоящего Положения.

3.12. Кредитная организация (головная кредитная организация банковской группы) определяет в документах, регламентирующих процедуры управления операционным риском, способы их проведения, перечисленные в настоящей главе Положения, с учетом требований главы 10 настоящего Положения.

3.13. Уполномоченное подразделение, определенное в соответствии с подпунктом 4.1.4 пункта 4.1 настоящего Положения, ежегодно осуществляет оценку эффективности выполнения процедур управления операционным риском кредитной организации (банковской группы), в том числе в соответствии с абзацем 16 пункта 1.1 приложения 1 к Указанию Банка России № 3624-У. Отчет о результатах оценки эффективности выполнения процедур управления операционным риском (в том числе на предмет их полноты и корректности) предоставляется уполномоченным подразделением на рассмотрение совету директоров (наблюдательному совету) и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы), в срок, установленный в документах кредитной организации (головной кредитной организации банковской группы).

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

4.1. Система управления операционным риском в кредитной организации, в дополнение к элементам, предусмотренным в абзацах 2-7, 10 пункта 1.3 настоящего Положения, включает следующие элементы.

4.1.1. Перечень банковских процессов кредитной организации, отнесенных к направлениям деятельности, с указанием их уровня критичности, функций подразделений-владельцев процессов (то есть подразделения, в чьи функциональные обязанности входит осуществление операций и сделок, поддерживаемых данным банковским процессом и ответственность за результаты выполнения данного банковского процесса, достижения целевых показателей банковского процесса), подразделений-участников процесса (другие структурные подразделения кредитной организации, выполняющие этапы банковского процесса).

По уровню критичности банковские процессы кредитной организации делятся на критически важные процессы, основные, обеспечивающие и прочие.

Критически важные банковские процессы обеспечивают выполнение банковских операций кредитной организации, указанных в пунктах 1-4, 9 статьи 5 Федерального закона от 2 декабря 1990 года № 395-1 «О банках и банковской деятельности» (Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 1998, № 31, ст. 3829; 1999, № 28, ст. 3459, ст. 3469; 2001, № 26, ст. 2586; № 33, ст. 3424; 2002, № 12, ст. 1093; 2003, № 27, ст. 2700; № 50, ст. 4855; № 52, ст. 5033, ст. 5037; 2004, № 27, ст. 2711; № 31, ст. 3233; 2005, № 1, ст. 18, ст. 45; № 30, ст. 3117; 2006, № 6, ст. 636; № 19, ст. 2061; № 31, ст. 3439; № 52, ст. 5497; 2007, № 1, ст. 9; № 22, ст. 2563; № 31, ст. 4011; № 41, ст. 4845; № 45, ст. 5425; № 50, ст. 6238; 2008, № 10, ст. 895; 2009, № 1, ст. 23; № 9, ст. 1043; № 18, ст. 2153; № 23, ст. 2776; № 30, ст. 3739; № 48, ст. 5731; № 52, ст. 6428; 2010, № 8, ст. 775; № 27, ст. 3432; № 30, ст. 4012; № 31, ст. 4193; № 47, ст. 6028; 2011, № 7, ст. 905; № 27, ст. 3873, ст. 3880; № 29,

ст. 4291; № 48, ст. 6728, ст. 6730; № 49, ст. 7069; № 50, ст. 7351; 2012, № 27, ст. 3588; № 31, ст. 4333; № 50, ст. 6954; № 53, ст. 7605, ст. 7607; 2013, № 11, ст. 1076; № 19, ст. 2317, ст. 2329; № 26, ст. 3207; № 27, ст. 3438, ст. 3477; № 30, ст. 4048; № 40, ст. 5036; № 49, ст. 6336; № 51, ст. 6683, ст. 6699; 2014, № 6, ст. 563; № 19, ст. 2311; № 26, ст. 3379, ст. 3395; № 30, ст. 4219; № 40, ст. 5317, ст. 5320; № 45, ст. 6144, ст. 6154; № 49, ст. 6912; № 52, ст. 7543; 2015, № 1, ст. 37, № 17, ст. 2473, № 27, ст. 3947, 3950; № 29, ст. 4355, 4357, 4385; № 51, ст. 7243; 2016, № 1, ст. 23; № 15, ст. 2050; № 26, ст. 3860; № 27, ст. 4294, 4295; 2017, № 14, ст. 2000; № 18, ст. 2661, 2669; № 25, ст. 3596; № 30, ст. 4456; № 31, ст. 4754, 4761, 4830; 2018, № 1, ст. 66; № 18, ст. 2560, 2576; № 22, ст. 3043; № 24, ст. 3400; № 27, ст. 3950; № 31, ст. 4852; № 32, ст. 5100, 5115; № 49, ст. 7524; № 53, ст. 8440) (далее – Федеральный закон № 395-1), включая процессы обеспечения переводов денежных средств (в том числе через банки-корреспонденты), ведение банковских счетов, бухгалтерский и управленческий учет, предоставление обязательной отчетности Банку России, процессы обеспечения ликвидности, операции на финансовых рынках, кассовые операции, онлайн сервисы дистанционного обслуживания и доступа к осуществлению банковских операций, процессов, обеспечивающих соблюдения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, №31, ст. 3451; 2009, № 48, ст. 5716; № 52, ст. 6439; 2010, № 27, ст. 3407; № 31, ст. 4173, 4196; №49, ст. 6409; № 52, ст. 6974; 2011, № 23, ст. 3263; № 31, ст. 4701; 2013, № 14, ст. 1651; № 30, ст. 4038; № 51, ст. 6683; 2014, № 23, ст. 2927; № 30, ст. 4217, 4243; 2016, № 27, ст. 4164; 2017, № 9, ст. 1276; № 27, ст. 3945; № 31, ст. 4772; 2018, № 1, ст. 82), «Трудового кодекса Российской Федерации» от 30 декабря 2001 года № 197-ФЗ (Собрание законодательства Российской Федерации, 2002, № 1, ст. 3; 2002, № 30, ст. 3014, 3033; 2003, № 27, ст. 2700; 2004, № 18, ст. 1690; № 35, ст. 3607; 2005, № 1, ст. 27; № 19, ст. 1752; 2006, № 27, ст. 2878; № 52, ст. 5498; 2007, № 1, ст. 34; № 17, ст. 1930; № 30, ст. 3808; № 41, ст. 4844; № 43, ст. 5084; № 49, ст. 6070; 2008,

№ 9, ст. 812; № 30, ст. 3613, 3616; № 52, ст. 6235, 6236; 2009, № 1, ст. 17, 21; № 19, ст. 2270; № 29, ст. 3604; № 30, ст. 3732, 3739; № 46, ст. 5419; № 48, ст. 5717; 2010, № 31, ст. 4196; № 52, ст. 7002; 2011, № 1, ст. 49; № 25, ст. 3539; № 27, ст. 3880; № 30, ст. 4586, 4590, 4591, 4596; № 45, ст. 6333, 6335; № 48, ст. 6730, 6735; № 49, ст. 7015, 7031; № 50, ст. 7359; 2012, № 10, ст. 1164, № 14, ст. 1553; № 18, ст. 2127; № 31, ст. 4325; № 47, ст. 6399; № 50, ст. 6954, 6957, 6959; № 53, ст. 7605; 2013, № 14, ст. 1666, 1668; № 19, ст. 2322, 2326, 2329; № 23, ст. 2866, 2883; № 27, ст. 3449, 3454, 3477; № 30, ст. 4037; № 48, ст. 6165; № 52, ст. 6986; 2014, № 14, ст. 1542, 1547, 1548; № 19, ст. 2321; № 23, ст. 2930; № 26, ст. 3405; № 30, ст. 4217; № 45, ст. 6143; № 48, ст. 6639; № 49, ст. 6918; № 52, ст. 7543, 7554; 2015, № 1, ст. 10, 42, 72; № 14, ст. 2022; № 18, ст. 2625; № 24, ст. 3379; №27, ст. 3991, 3992; № 29, ст. 4356, 4359, 4363, 4368; № 41, ст. 5639; 2016, № 1, ст. 11, 54; № 18, ст. 2508; № 27, ст. 4169, 4172, 4205, 4238, 4280, 4281; 2017, № 1, ст. 46; № 18, ст. 2661; № 25, ст. 3594; № 27, ст. 3929, 3936; № 31, ст. 4804, 4805; № 49, ст. 7331; № 52, ст. 7923; 2018, № 1, ст. 45, 86; № 7, ст. 968; № 30, ст. 4542; № 32, ст. 5097, 5108; № 41, ст. 6193; № 42, ст. 6374; № 53, ст. 8468), Федерального закона № 395-1, а также другие банковские процессы по усмотрению кредитной организации, прерывание функционирования которых по времени, сверх установленных кредитной организацией пороговых значений, оказывает влияние на выполнение стратегии развития и нарушения обязательств перед клиентами и контрагентами кредитной организации.

Основные банковские процессы обеспечивают выполнение всех банковских операций, предусмотренных статьей 5 Федерального закона № 395-1, не отнесенных кредитной организацией к критически важным банковским процессам, и других банковских операций и услуг, объем операций которых формирует объем общих валовых расходов (доходов) более 5% от валового дохода кредитной организации.

Обеспечивающие и прочие банковские процессы, не отнесенные к критически важным банковским процессам или основным банковским процессам.

4.1.2. Политику (положение) по управлению операционным риском и документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования системы управления операционным риском.

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

Кредитные организации-участники банковской группы должны согласовывать документы по структуре и организации в кредитной организации системы управления операционным риском, а также документы, указанные в подпункте 4.1.2 настоящего пункта Положения, с головной кредитной организацией банковской группы.

4.1.4. Порядок оценки кредитной организацией и (или) внешними экспертами эффективности 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 (например, Служба внутреннего аудита), уполномоченное проводить оценку эффективности функционирования системы управления операционным риском и ее элементов, в том числе оценку эффективности выполнения принятых в кредитной организации процедур по управлению операционным риском (далее – уполномоченное подразделение), порядок привлечения для оценки эффективности функционирования системы управления операционным риском внешних экспертов.

4.1.5. Система мер, в дополнение к мерам, указанным в пункте 4.6 приложения 1 к Указанию Банка России №3624-У, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска, включающая 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:

встраивание дополнительных способов контроля, например, указанных в пунктах 1.10, 1.11, 1.15, 1.17, 1.18, 1.28 приложения 3 к настоящему Положению, в шаги (единичные операции) банковских процессов, в которых выявлены операционные риски;

исключение конфликта интересов;

повышение эффективности процедур контроля в банковских процессах, документирования их результатов;

другие меры, разрабатываемые кредитной организацией в зависимости от вида и характеристик банковского процесса, в том числе и из списка мер, направленных на ограничение размера потерь от событий операционного риска.

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

ведение пороговых значений по материальности и существенности, в отношении полномочий принятия решений и лимитов операционного риска, контроля за соблюдением полномочий;

внедрение элементов автоматизации участков банковских процессов, где выявлены операционные риски по причине ошибок работников;

разработку планов по обеспечению непрерывности критически важных банковских 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, с учетом влияния внешних факторов, влияющих на критически важный банковский процесс;

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, например, с использованием переноса риска на участников финансового рынка, например, страхования;

правовое сопровождение судебных исков со стороны третьих лиц;

юридическую проработку процессов, договоров и документации кредитной организации;

другие меры, направленные на ограничение размера потерь от событий операционного риска.

Кредитная организация (головная кредитная организация банковской группы), в зависимости от масштаба и характера деятельности, определяет в документах систему мер, направленную на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска.

Головная кредитная организация банковской группы должна обеспечить соответствие указанных мероприятий во всех дочерних кредитных организациях и других участниках банковской группы.

4.1.6. Способы мотивации работников к участию в управлении операционным риском, в части:

инициативного информирования о возможных операционных рисках и выявленных работниками кредитной организации (участника банковской группы) событий операционного риска;

выполнения процедур управления операционным риском, указанных в главе 3 настоящего Положения;

направления предложений по мерам повышения качества системы управления операционным риском;

реализации мер, указанных в подпункте 4.1.5 пункта 4.1 настоящего Положения;

других форм участия работников кредитной организации.

Кредитная организация (головная кредитная организация банковской группы) определяет в документах способы мотивации работников кредитной организации к участию в управлении операционным риском, включающие показатели соблюдения сигнальных и контрольных значений контрольных показателей уровня операционного риска, установленных в соответствии с главой 5 настоящего Положения, а также категории работников, на которые распространяются способы мотивации, указанные в настоящем пункте.

4.2. Кредитная организация (головная кредитная организация банковской группы) формирует отчеты по операционному риску, включаемые в состав отчетности ВПОДК в соответствии с пунктом 6.2 Указания Банка России № 3624-У.

В дополнение к отчетам, формируемым в соответствии с пунктом 6.2 Указания Банка России № 3624-У, кредитная организация (головная кредитная организация банковской группы) формирует следующие отчеты:

об управлении операционным риском, включающий информацию о событиях операционного риска и потерях, за исключением информации о событиях риска ИБ, в соответствии с абзацем 2 подпункта 4.2.1.2 настоящего пункта Положения;

о событиях риска ИБ в соответствии с абзацем 3 подпункта 4.2.1.2 настоящего пункта Положения;

о фактических сигнальных и контрольных значениях контрольных показателей уровня операционного риска, установленных в кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями главы 5 настоящего Положения;

об управлении операционным риском за год в соответствии с подпунктом 4.2.1.3 настоящего пункта Положения.

4.2.1 Подразделение, ответственное за организацию управления операционным риском, формирует отчеты по операционному риску в соответствии с абзацем 2 пункта 4.2 настоящего Положения на ежеквартальной и ежегодной основе и обеспечивает ежедневное направление информации (предоставление доступа к информации) руководителю службы управления рисками.

4.2.1.1. Подразделение, ответственное за организацию управления операционным риском, ежедневно предоставляет руководителю службы управления рисками информацию о значительных и крупных событиях операционного риска, зарегистрированных в базе событий за отчетный день, и обстоятельств их возникновения, их влияния на соблюдение показателей объема операционного риска, в соответствии с пунктом 4.5 настоящего Положения, другой информации.

Кредитная организация (головная кредитная организация банковской группы) определяет в документах порядок информирования руководителя службы управления рисками и критерии значимости событий операционного риска, включаемых в ежедневное информирование по операционному риску.

Кредитная организация (головная кредитная организация банковской группы) для целей снижения трудозатрат определяет порядок автоматизированного формирования информации из базы событий и ее направления в электронном виде руководителю службы управления рисками, а также организацию прямого доступа к базе событий (либо другому информационному ресурсу) для самостоятельного просмотра (выгрузки) информации работниками службы управления рисками.

4.2.1.2. Подразделение, ответственное за организацию управления операционным риском, ежеквартально формирует и направляет руководителю службы управления рисками, коллегиальному исполнительному органу кредитной организации, следующие отчеты:

об управлении операционным риском, включающий информацию о событиях операционного риска и потерях, за исключением информации о событиях риска ИБ, в кредитной организации и банковской группы, содержащий информацию о событиях операционного риска и потерях кредитной организации (головной кредитной организации банковской группы и участников банковской группы) в разрезе классификационных критериев в соответствии с главой 2 настоящего Положения и отдельных видов операционного риска в соответствии с пунктом 1.4 настоящего Положения, за исключением событий риска ИБ, содержащий информацию, указанную в подпункте 4.2.2 настоящего пункта Положения, о результатах проведенных процедур управления операционным риском, в том числе, о результатах количественной и качественной оценки операционного риска, выбранных способов реагирования, результатах мониторинга операционного риска, результатах выполнения мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска.;

о событиях риска ИБ (включая киберриск);

о фактических сигнальных и контрольных значениях контрольных показателей уровня операционного риска (включая контрольные показатели риска ИБ в соответствии с подпунктом 2.2 пункта 2 приложения 4 к настоящему Положению).

Кредитная организация (головная кредитная организация банковской группы) включает в отчеты за четвертый квартал отчетного года, помимо данных за четвертый квартал, информацию за отчетный год.

4.2.1.3. Подразделение, ответственное за организацию управления операционным риском, ежегодно формирует и направляет руководителю службы управления рисками и коллегиальному исполнительному органу кредитной организации отчет об управлении операционным риском за год, содержащий сведения о мероприятиях и планах работ, планируемых к

применению в целях снижения негативного влияния риска, информацию, указанную в абзаце 2 подпункта 4.2.1.2 настоящего пункта Положения.

Кредитная организация (головная кредитная организация банковской группы) устанавливает в документах порядок предоставления информации на рассмотрение совета директоров (наблюдательного совета), в рамках которого осуществляется рассмотрение отчета об управлении операционным риском за год советом директоров (наблюдательным советом).

4.2.2. Информация о событиях реализации операционного риска включается в отчеты, указанные в подпункте 4.2.1.2 настоящего пункта Положения, в разрезе направлений деятельности и банковских процессов, типов событий и источников риска, в том числе отдельно по видам риска, и содержит 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 в разрезе прямых, косвенных потерь и потерь клиентов и третьих лиц, с начала года до отчетной даты и в отчетном периоде;

сумма прямых, косвенных потерь, потерь клиентов и третьих лиц от реализации событий операционного риска во всей банковской группе и в разрезе участников банковской группы, включая головную кредитную организацию банковской группы, с начала года до отчетной даты и в отчетном периоде, в разрезе направлений деятельности, банковских процессов, типов событий, в соответствии с пунктом 2.11 настоящего Положения;

сумма прямых, косвенных потерь, потерь клиентов и третьих лиц от реализации событий операционного риска от других связанных с кредитной организацией юридических и физических лиц, не входящих в состав банковской группы, с начала года до отчетной даты и в отчетном периоде;

сумма прямых, косвенных потерь, потерь клиентов и третьих лиц в части затрат на восстановление деятельности, в разрезе направлений деятельности и

составляющих их банковских процессов, типов событий, за отчетный период, нарастающим итогом до отчетной даты и в отчетном периоде;

сумма прямых потерь регуляторного риска, связанных с реализацией операционного риска и включаемых в состав валовых потерь от реализации событий операционного риска в соответствии с пунктом 6.10 настоящего Положения;

максимальная величина прямых, косвенных потерь и потерь клиентов 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 составляющих их банковских процессов;

максимальная сумма прямых, косвенных потерь и потерь клиентов от пяти крупнейших (по сумме потерь) событий из тех, которые были зафиксированы у кредитной организации с начала года до отчетной даты и в отчетном периоде в разрезе направлений деятельности и банковских процессов;

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

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

сумма чистых потерь, то есть сумма потерь с учетом суммы возмещения, которая была отражена 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, банковских процессов и типов событий;

среднеквадратичное отклонение (сигма) величины прямых потерь по группам событий реализации операционного риска в разрезе направлений деятельности, банковских процессов и типов событий за отчетный период, нарастающим итогом за 3, 6, 9 месяцев, 1 год;

распределение потерь от событий операционного риска по группам (до 20 тысяч рублей (в случае если кредитная организация регистрирует события операционного риска с суммой меньше 20 тысяч рублей), от 20 тысяч до 100 тысяч рублей; от 100 тысяч до 350 тысяч рублей, от 350 тысяч рублей до 700 тысяч рублей, от 700 тысяч до 1 400 тысяч рублей, от 1 400 тысяч рублей и выше).

4.2.3 Коллегиальный исполнительный орган кредитной организации рассматривает в установленные сроки (но не позднее двадцати рабочих дней с момента получения) отчеты по операционным рискам кредитной организации и дает поручения по разработке мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска, с указанием ответственных за реализацию мер подразделений и сроков выполнения.

Отчеты по операционным рискам должны храниться в кредитной организации не менее десяти лет со дня рассмотрения коллегиальным исполнительным органом кредитной организации.

4.3. Кредитная организация (головная кредитная организация банковской группы), признаваемая крупным банком в соответствии с пунктом 9.1 настоящего Положения, дополнительно обеспечивает соблюдение следующих требований.

4.3.1 Кредитная организация (головная кредитная организация банковской группы), признаваемая крупным банком в соответствии с пунктом 9.1 настоящего Положения, устанавливает в документах требования к информационной системе, обеспечивающей управление операционным риском и включающей автоматизацию ведения базы событий и процедур управления операционным риском.

Кредитная организация (головная кредитная организация банковской группы), признаваемая крупным банком в соответствии с пунктом 9.1 настоящего Положения, в зависимости от характера и масштаба осуществляемых операций и действующих банковских процессов, обеспечивает информационный обмен 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 операционного риска.

4.3.2. Кредитная организация (головная кредитная организация банковской группы), признаваемая крупным банком в соответствии с пунктом 9.1 настоящего Положения, устанавливает в документах требования к управлению модельным риском, связанным с реализацией операционного риска. Кредитная организация (головная кредитная организация банковской группы) обеспечивает соблюдение процедур управления указанным видом риска, который включает в себя:

ошибки, недостоверность и неполнота данных, использованных при разработке, проверке, адаптации, приемке и применении моделей;

некорректное применение методик и технологий моделирования, ошибки в реализации бизнес-логики работы моделей, в том числе в связи с некачественной постановкой задачи на разработку, применение необоснованных допущений и экспертных суждений при разработке моделей;

ошибки в процессах регистрации, учета и отчетности по моделям, отсутствие и неполнота документации по моделям;

ошибки в процессе внутренней валидации моделей, в том числе. связанные с некорректной реализацией статистических тестов по моделям, некорректной интерпретацией результатов валидации;

ошибки во внедрении моделей в промышленную эксплуатацию, в том числе связанные с некорректной имплементацией программного кода в автоматизированные системы кредитной организации;

ошибки применения моделей для целей принятия управленческих и бизнес-решений в кредитной организации, в том числе связанные с использованием моделей для нецелевых объектов и клиентских сегментов, некорректным заполнением входных данных для работы моделей, некорректной интерпретацией результатов работы моделей для целей принятия решений.

4.4. Уполномоченное подразделение кредитной организации в соответствии с подпунктом 4.1.4 пункта 4.1 настоящего Положения ежегодно осуществляет оценку эффективности функционирования системы управления операционным риском, включающую оценку:

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

правильности определения вида и величины потерь от событий операционного риска;

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

корректности проведенных оценок величины потерь от операционного риска и величины потерь, в соответствии с пунктом 3.4 настоящего Положения;

системы мер, разрабатываемой в соответствии с подпунктом 4.1.5 пункта 4.1 настоящего Положения;

эффективности мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска.

Кредитная организация (головная кредитная организация банковской группы) устанавливает порядок информирования уполномоченным подразделением коллегиального исполнительного органа кредитной организации (головной кредитной организации банковской группы), должностного лица, отвечающего за управление рисками, должностного лица,

отвечающего за обеспечение информационной безопасности, подразделения, ответственного за организацию управления операционным риском, о выявленных недостатках в системе управления операционным риском в кредитной организации (банковской группе, участнике банковской группы) и действиях, предпринятых для их устранения, в том числе в соответствии с пунктом 1.1 приложения 1 к Указанию Банка России № 3624-У.

4.5. Кредитная организация (головная кредитная организация банковской группы) для целей контроля за принятым в кредитной организации объемом операционного риска, в соответствии с пунктом 3.4 Указания Банка России № 3624-У, разрабатывает и устанавливает показатели объема операционного риска в разрезе направлений деятельности и составляющих их банковских процессов, которые формируются на основе следующих показателей, характеризующих объемы операций, подверженных операционному риску за определенный период (день, неделя, месяц, квартал, год):

количество сделок, операций, транзакций;

объем сделок, операций, транзакций в денежном выражении в рублевом эквиваленте;

количество платежей, осуществленных через корреспондентский счет кредитной организации и другие корреспондентские счета платежных систем;

валовый доход, определяемый в соответствии с пунктом 3 Положения Банка России от 3 сентября 2018 года № 652-П «О порядке расчета размера операционного риска», зарегистрированного Министерством юстиции Российской Федерации 19 ноября 2018 года № 52705, 19 декабря 2018 года № 53050 (далее – Положение Банка России № 652- П);

обороты по счетам бухгалтерского учета;

другие показатели.

Кредитная организация (головная кредитная организация банковской группы) соотносит показатели, характеризующие объем операций, с зарегистрированными в базе событий потерями и определяет показатели

объема операционного риска, порядок контроля которых устанавливается в документах кредитной организации.

4.6. Подразделение, ответственное за организацию управления операционным риском, проводит регулярный (не реже одного раза в год) анализ необходимости пересмотра требований политики управления операционным риском в зависимости от характера и масштаба осуществляемых операций, действующих банковских процессов, изменяющихся факторов внешней среды, результатов процедур управления операционным риском, результатов оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, изменений в стратегии управления рисками и капиталом, и выносит результаты анализа на рассмотрение коллегиальным исполнительным органом кредитной организации для принятия решения о необходимости внесений изменений в документы, указанные в подпунктах 4.1.2 и 4.1.3 пункта 4.1 настоящего Положения.

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, порядок установления количественных и качественных контрольных показателей уровня операционного риска, в том числе устанавливает целевые значения этих показателей: значение показателя, при нарушении которого проводится ежедневный мониторинг значений показателя и реализация мероприятий, направленных на устранение превышения фактического значения данного показателя над предельно допустимым значением показателя (далее - сигнальное значение), и предельно допустимое значение показателя, при нарушении которого информация доводится до совета директоров (наблюдательного совета) и применяются

меры реагирования, которые описаны в документах кредитной организации (головной кредитной организации банковской группы) в соответствии с пунктом 5.4 настоящего Положения (далее - контрольное значение), а также контроля их соблюдения.

5.2. Совет директоров (наблюдательный совет) кредитной организации (головной кредитной организации банковской группы):

утверждает сигнальные и контрольные значения количественных контрольных показателей уровня операционного риска на плановый годовой период как в целом по кредитной организации (по банковской группе), так и в разрезе направлений деятельности и структурных подразделений-владельцев банковских процессов (участников банковской группы), которые ежегодно пересматриваются и актуализируются в рамках регулярных процедур управления рисками, в соответствии с абзацем 1 пункта 3.5 Указания Банка России № 3624-У, в том числе по результатам оценки эффективности функционирования системы управления операционным риском, в соответствии с пунктом 4.4 настоящего Положения;

обеспечивает контроль за фактическими значениями сигнальных и контрольных значений контрольных показателей;

обеспечивает реагирование кредитной организации в случае превышения сигнальных и контрольных значений контрольных показателей.

5.3. Подразделение, ответственное за организацию управления операционным риском, проводит расчет сигнальных и контрольных значений контрольных показателей на основе статистических данных о событиях операционного риска за период не менее десяти лет в соответствии с установленным в документах кредитной организации (головной кредитной организацией банковской группы) порядком.

В случае если период ведения базы событий меньше десяти лет, расчет производится на основе фактически имеющегося периода наблюдений с последующим добавлением данных за новые годы, по мере их накопления, вплоть до полных десяти лет.

В случае отсутствия данных за полные десять лет кредитная организация (головная кредитная организация банковской группы) определяет методику учета недостающих данных в документах.

Подразделение, ответственное за организацию управления операционным риском, оформляет расчет и обоснование сигнальных и контрольных значений контрольных показателей в виде мотивированного суждения и включает в состав материалов, выносимых данным подразделением на рассмотрение коллегиальным исполнительным органом кредитной организации при утверждении (пересмотре) политики управления операционным риском.

5.4. Кредитная организация (головная кредитная организация банковской группы) определяет в документах порядок действий, роли и ответственность органов управления и структурных подразделений кредитной организации (головной кредитной организации банковской группы), должностных лиц в соответствии с пунктом 1.1 приложения 1 к Указанию Банка России № 3624-У, а также определяет систему мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска или пересмотр сигнальных и контрольных значений контрольных показателей, в том числе порядок информирования совета директоров (наблюдательного совета) кредитной организации (головной кредитной организации банковской группы).

Глава 6. **Требования к ведению базы событий**

6.1. Кредитная организация (головная кредитная организация банковской группы) ведет на постоянной основе базу событий в соответствии с требованиями настоящей главы Положения.

6.2. Кредитная организация (головная кредитная организация банковской группы) определяет в документах, ведется ли база событий консолидировано по банковской группе или раздельно по участникам банковской группы. В случае раздельного ведения базы событий участники банковской группы на ежемесячной основе представляют данные о событиях

операционного риска и потерях в головную кредитную организацию банковской группы в целях расчета капитала банковской группы, необходимого на покрытие операционного риска и соблюдения ВПОДК банковской группы, в соответствии с Указанием Банка России № 3624-У.

Головная кредитная организация банковской группы, в целях предоставления отчетности Банку России, устанавливает в документах правила соотнесения классификации событий операционного риска участников банковской группы, ведущих учет событий операционного риска по другим классификационным критериям, с требованиями главы 2 настоящего Положения и определяет порядок предоставления отчетности участников банковской группы с учетом правил соотнесения классификации.

Головная кредитная организация банковской группы определяет в документах другие формы отчетности участников банковской группы по операционному риску.

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

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

Кредитная организация (головная кредитная организация банковской группы) обеспечивает наличие в базе событий подробной информации о причинах и обстоятельствах реализованных событий операционного риска.

6.5. Порог регистрации выявленных событий операционного риска в базе событий устанавливается в зависимости от величины потерь и типа событий:

для событий операционного риска, относящихся к типам, указанным в подпунктах 2.7.1, 2.7.2 пункта 2.7 настоящего Положения, порог регистрации в базе событий не устанавливается;

для событий операционного риска, относящихся к потерям клиентов, произошедших не по вине клиентов, порог регистрации в базе событий не устанавливается;

для других типов событий операционного риска порог регистрации в базе событий составляет не более 20 000 рублей (прямых и непрямых потерь).

Кредитная организация (головная кредитная организация банковской группы) может установить порог регистрации событий операционного риска, не превышающий 20 000 рублей, либо не устанавливать порог.

В случае если событие операционного риска привело только к качественным потерям, оценка значимости которых в соответствии с абзацем 10 подпункта 2.11.2.2 пункта 2.11 настоящего Положения составляет «средние» или ниже, кредитная организация (головная кредитная организация банковской группы) определяет в документах требования к регистрации таких событий в базе событий.

6.6. База событий кредитной организации (участников банковской группы, в случае раздельного ведения базы событий) должна содержать следующую информацию:

уникальный порядковый идентификационный номер события операционного риска;

идентификатор группы событий операционного риска (в случае если события объединены в группу) в соответствии с пунктом 6.15 настоящего Положения;

информацию о дате, когда событие операционного риска было зарегистрировано в базе событий («дата регистрации»);

информацию о времени, когда событие операционного риска было зарегистрировано в базе событий, в случае программно-аппаратной фиксации событий;

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

информацию о времени, когда событие операционного риска произошло или впервые началось, в случае программно-аппаратной фиксации событий и для событий риска ИБ;

информацию о дате (и времени, в случае, когда характер события это предусматривает), когда кредитной организации стало известно о событии операционного риска («дата обнаружения (дата выявления)»);

информацию о дате (и времени, для событий риска ИБ) окончания события операционного риска («дата окончания события»), в случае если наличие такой информации определяется характером события операционного риска;

статус события операционного риска (то есть, оценка потерь от события операционного риска завершена (не завершена), при этом, кредитная организация (головная кредитная организация банковской группы) определяет виды статусов события);

подразделение, в котором произошло событие операционного риска;

подразделение, выявившее событие операционного риска;

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

категории источников операционного риска, в соответствии с пунктом 2.3 настоящего Положения;

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

тип события, в соответствии с пунктом 2.7 настоящего Положения;

вид операционного риска (в случае если событие отнесено к одному из видов операционного риска, в соответствии с пунктом 1.4 настоящего Положения);

связь с другими видами риска (кредитный, рыночный, ликвидности, стратегический, репутационный и другие), при наличии такой связи, при этом указывается:

является ли другой риск источником события операционного риска;

является ли другой риск следствием события операционного риска;

идентификатор связанного события операционного риска (идентификатор цепочки событий), в случае если такая связь установлена, при этом указывается:

является ли событие операционного риска источником другого события операционного риска;

является ли событие операционного риска следствием другого события операционного риска;

дополнительная классификация типа события операционного риска в зависимости от вида риска;

направление деятельности, в соответствии с пунктом 2.10 настоящего Положения;

банковский процесс, согласно перечню (реестру) процессов, принятых в документах кредитной организации;

шаг (единичная операция) банковского процесса, согласно принятым в кредитной организации правилам описания банковских процессов (при наличии);

информационная система (в случае если задействована на выполнении шага (единичной операции) банковского процесса).

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

вид потери, в соответствии с пунктом 2.11 настоящего Положения;

признак связи потери с другим риском (при наличии такой связи), который не будет включаться в состав валовых потерь, в соответствии с пунктом 6.7 настоящего Положения;

величину потери от события операционного риска, определяемую в соответствии с документами кредитной организации, в рублях (например, в случае прямых потерь – сумма бухгалтерской записи (далее – запись) по счетам бухгалтерского учета, в случае непрямых потерь – оценочное значение);

дату учета потери, то есть дату отражения операционной потери на счетах бухгалтерского учета (например, для событий правового риска датой учета являются дата создания резерва-оценочного обязательства некредитного характера и даты отражения в бухгалтерском учете других связанных с этим обстоятельством расходов, для событий операционного риска, связанных с кредитным риском датой учета является дата создания (изменения) резерва на возможные потери по ссудам);

информацию о записи (записях) в бухгалтерском учете суммы прямой потери (суммы косвенной потери при возможности ее определения);

экспертную оценку качественной потери, в соответствии с подпунктом 2.11.2.2 пункта 2.11 настоящего Положения, в случае регистрации наличия качественной потери для события операционного риска, в результате которого возникла данная потеря;

обоснование величины потери (для косвенных потерь меньше 100 000 рублей, обоснование не заполняется);

агрегированная сумма валовых потерь в рублях;

агрегированная сумма прямых потерь в рублях;

агрегированная сумма косвенных потерь в рублях;

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

мероприятия, осуществленные кредитной организацией в целях получения возмещения по понесенным потерям в результате события операционного риска;

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

признак связи возмещения с компенсацией конкретного вида потерь от реализации события операционного риска, в соответствии с пунктом 2.11 настоящего Положения;

сумму возмещений в рублях;

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

информацию о записи в бухгалтерском учете суммы возмещения;

источники получения возмещения (от страховой компании, входящей в банковскую группу, от страховой компании, не входящей в банковскую группу, от связанных с кредитной организацией или участниками банковской группы лиц, от контрагента, от третьих лиц, от работников кредитной организации);

сумму чистых (фактических) потерь (после учета возмещения, в соответствии с требованиями пункта 6.18 настоящего Положения) с учетом правил зачета возмещений;

сумму потерь клиентов и третьих лиц от события операционного риска, в рублях.

В случае если сумма потерь и возмещений отражается в валюте, отличной от рубля, то пересчет в рубли отражается в базе событий по официальному курсу иностранной валюты по отношению к рублю, установленный Банком России в соответствии с пунктом 15 статьи 4 Федерального закона № 86-ФЗ (далее – курс иностранной валюты, установленный Банком России), на дату отражения в бухгалтерском учете кредитной организации.

Кредитная организация (головная кредитная организация банковской группы) определяет в документах другие поля базы событий.

6.7. Кредитная организация (головная кредитная организация банковской группы) ежемесячно на отчетную дату определяет величину валовых потерь (как сумму потерь от реализации операционного риска до учета возмещения) от событий операционного риска со статусом «оценка потерь не завершена» от начала регистрации события операционного риска в базе событий и от начала календарного года (в случае если событие операционного риска реализовалось ранее текущего календарного года) нарастающим итогом. Также в расчет включаются потери от событий операционного риска, статус которых был переведен в «оценка потерь завершена» в течение отчетного месяца.

Головная кредитная организация банковской группы для целей расчета величины валовых потерь по банковской группе осуществляет перерасчет суммы валовых потерь и последующих возмещений от событий операционного риска, произошедших у иностранных участников банковской группы, ведущих учет событий операционного риска в иностранной валюте, в рубли по курсу иностранной валюты, установленному Банком России, на отчетную дату, с последующим ежемесячным перерасчетом на отчетную дату.

6.7.1. В расчет величины валовых потерь включаются:

сумма прямых потерь от события операционного риска в соответствии с подпунктом 2.11.1 пункта 2.11 настоящего Положения, включая обесценение, списание активов, отраженные на счетах бухгалтерского учета кредитной организации;

корректировка стоимости потерь, не отраженных в бухгалтерском учете в течение текущего календарного года, связанных с перерасчетом стоимости потерь от реализации события операционного риска прошлого периода в случае если отражение в бухгалтерском учете потерь длится более одного календарного года (далее – «распределенные во времени потери»), при этом, в

случае такой корректировки, потери рассчитываются в корреспонденции со счетами расходов текущего года;

потери по событиям операционного риска, которые вызывают временное искажение финансовой отчетности кредитной организации за определенный отчетный период (календарный год), но которые могут быть полностью скорректированы в дальнейшем (например, при завершении расчетов, создании исправительных записей в бухгалтерском учете и переоценки справедливой стоимости финансовых инструментов, далее – временные потери).

Кредитная организация (головная кредитная организация банковской группы) определяет в документах порядок учета размера валовых потерь, в том числе для целей расчета показателя, указанного в абзаце 8 пункта 1 приложения 4 к настоящему Положению, позволяющий точно определять уровень операционного риска.

6.7.2 Кредитная организация определяет в документах порядок идентификации потерь и возмещений с указанием дат учета, сумм и реквизитов записей в разрезе всех событий, повлекших потери.

6.7.3. В валовые потери не включаются:

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 завершения оценки потерь от реализации операционного риска (модернизация, совершенствование, меры по предотвращению риска, по улучшению качества банковских процессов, по оценке рисков и расширению функционала по управлению рисками);

выплата страховых премий;

расходы, связанные с доначислением резервов на возможные потери по ссудам по событиям операционного риска, повлекшим реализацию кредитного риска на конкретных ссудах и приравненной к ним задолженности.

6.8. По одному и тому же событию операционного риска выявляются и учитываются в базе событий все виды произошедших потерь. Каждая потеря отражается в базе событий отдельной записью с указанием номера записи (идентификатора записи), датой учета и с пометкой о связи с другим риском.

Кредитная организация (головная кредитная организация банковской группы) приводит перечень всех записей одного вида потери от события операционного риска в поле описание события либо в виде вложения, со списком всех записей в разбивке по суммам.

6.9. Кредитная организация (головная кредитная организация банковской группы) ведет учет потерь от событий всех видов операционного риска (например, риск ИБ, правовой риск) и других нефинансовых рисков как в составе общей базы событий, так и раздельно. При этом кредитная организация (головная кредитная организация банковской группы) 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.

6.10. В случае если кредитная организация ведет отдельную базу событий регуляторного риска, прямые потери от его реализации, связанные с реализацией операционного риска, включаются ежемесячно на отчетную дату в валовые потери от событий операционного риска с учетом исключения пропусков и дублирования потерь, связанных с раздельным ведением баз событий.

6.11. В случае если у события операционного риска потери распределены по разным учетным периодам (годам), данные потери в базе событий должны быть отнесены к годам их отражения на счетах бухгалтерского учета, в соответствии с пунктом 6.10 настоящего Положения.

6.12. Кредитная организация (головная кредитная организация банковской группы) разрабатывает специальные критерии для определения данных о потерях, вызванных единичными событиями реализации

операционного риска или однородными событиями, произошедшими в течение некоторого времени («группа событий»).

Кредитная организация (головная кредитная организация банковской группы) определяет в документах критерии однородности событий для целей их группировки (например, события операционного риска группируются в одну группу, в случае если у них одинаковый источник риска, банковский процесс, один и тот же шаг (единичная операция) банковского процесса, тип события, другие критерии группировки, а период времени возникновения до 48 часов). Группировка событий должна быть предметом оценки, проводимой уполномоченным подразделением.

6.13. Возмещение является отдельной записью в блоке возмещений базы событий у одного события операционного риска, связанное с регистрацией в бухгалтерском учете компенсации потери от события операционного риска и отраженное на счетах бухгалтерского учета в виде записи по счетам доходов (прибылей), обратной записи, другой записи с указанием номера записи (идентификатора записи), даты записи.

6.14. Кредитная организация (головная кредитная организация банковской группы) приводит перечень всех записей одного вида возмещения от события операционного риска в поле описание события либо в виде вложения, со списком всех записей в разбивке по суммам.

6.15. Виды возмещений:

возмещения, полученные в судебном порядке;

возмещения, полученные во внесудебном порядке по соглашению сторон;

получение страховой выплаты от одной или нескольких страховых компании;

компенсации от третьих лиц;

компенсации от других источников;

восстановление резерва на возможные потери по ссудам;

восстановление резерва некредитного характера.

6.16. Кредитная организация определяет порядок контроля за своевременностью учета возмещения по потерям от событий операционного риска.

6.17. Кредитные организации должны учитывать в базе событий отдельно валовые потери и потери за вычетом возмещения. Возмещение используется для уменьшения потерь только после того, как платеж получен кредитной организацией и отражен на счетах бухгалтерского учета. Дебиторская задолженность не является возмещением.

В случае поступления возмещения от третьего лица, а не внутренней записью кредитной организации, в базе событий указывается наименование третьего лица и его характеристики (например, страховая компания, контрагент, связано ли оно с кредитной организацией или банковской группой).

К зачету сумм возмещения не принимаются следующие виды возмещений:

возмещения, полученные от страховых компаний, входящих в банковскую группу (за исключением, в случае если поступление возмещения от страховой компании, входящей в банковскую группу, получено в рамках перестрахования рисков от страховых брокеров, не входящих в банковскую группу);

возмещения от связанных с кредитной организацией или участниками банковской группы лиц, акционеров, бенефициаров;

компенсации от других физических и юридических лиц или организаций, способных оказать влияние на деятельность кредитной организации.

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

6.18. Чистые (фактические) потери определяются как потери после вычета суммы возмещения с учетом требований пункта 6.17 настоящего Положения.

6.19. В случае корректировки потерь и возмещений в базе событий предыдущее значение не меняется, а добавляется новое поле с новым значением (либо должна быть обеспечена сохранность предыдущих значений).

Информация о записях в базе событий подлежит ежегодной независимой оценке, проводимой уполномоченным подразделением, ответственным за проведение оценки эффективности системы управления операционным риском.

6.20. Кредитная организация (головная кредитная организация банковской группы) обеспечивает сохранность всех записей в базе событий. Любое исправление записей фиксируется с указанием фамилии, имени, отчества (при наличии) работника, сделавшего исправление, дату и основание. Корректность исправления записи, в соответствии с указанным основанием, подлежит верификации.

6.21. Кредитная организация (головная кредитная организация банковской группы) в документах устанавливает перечень лиц кредитной организации с персональной ответственностью за несоблюдение требований документов по ведению базы событий, в том числе указывает в документах:

лиц, ответственных за ведение базы событий;

лиц, предоставляющих информацию для базы событий;

лиц, определяющих потери, занесенные в базу событий;

лиц, ответственных 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) определяет порядок управления риском ИБ, как риском реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе применения технологических и других мер, недостатками программного обеспечения автоматизированных систем и приложений, а также несоответствия указанных процессов характеру и (или) масштабам деятельности кредитной организации, требованиям нормативных актов Банка России, разработанных в рамках законодательства Российской Федерации о техническом регулировании и стандартизации.

7.2. Риск ИБ включает в себя:

риск преднамеренного воздействия работников кредитной организации, третьих лиц, внутренних (в том числе с применением компонентов иностранного производства) 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, в том числе путем реализации компьютерных атак (далее – киберриск);

риск непреднамеренного воздействия работников кредитной организации, третьих лиц, внутренних (в том числе с применением компонентов иностранного производства) и (или) сторонних информационных систем, в том числе бездействия или несвоевременного реагирования уполномоченных работников кредитной организации на угрозы, а также внешних факторов, приведший к несанкционированному распространению, изменению, удалению данных и другой цифровой информации и (или) структуры данных, параметров и характеристик систем (в том числе программного кода) и режима доступа;

другие 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 определяется второй уровень классификации источников:

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

уязвимость (как недостатки информационной системы или ее компонентов, обусловливающие возможность реализации угроз защиты данных и обрабатываемой цифровой информации), посредством которой реализована угроза.

7.4. Фактическая реализация риска ИБ, в том числе киберриска, обусловленная источниками (угрозами, уязвимостями) риска ИБ, инцидентами защиты информации, инцидентами, связанными с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, вследствие которых возникли прямые и непрямые потери кредитной организации и потери клиентов (далее – событие риска ИБ) фиксируется в базе событий с присвоением признака реализации данного вида риска, в соответствии с пунктом 6.6 настоящего Положения.

Негативное влияние риска ИБ проявляется в виде потерь, перечисленных в пункте 4 приложения 2 к настоящему Положению.

7.5. Кредитная организация (головная кредитная организация банковской группы) определяет в документах порядок ведения базы событий риска ИБ (например, как в общей базе событий, так и в отдельной базе событий риска ИБ). В случае если кредитная организация ведет отдельную базу событий риска ИБ, структурному подразделению (работникам), ответственному (ответственным) за организацию и контроль обеспечения защиты информации (далее – служба информационной безопасности) необходимо соблюдать требования к определению и классификации событий

риска ИБ, в соответствии с пунктами 2.3 - 2.12 настоящего Положения и требованиями к ведению базы событий в соответствии с пунктами 6.6 – 6.22 настоящего Положения.

7.6. Кредитная организация (головная кредитная организация банковской группы) классифицирует события риска ИБ в соответствии с главой 2 настоящего Положения с использованием элементов дополнительной классификации по источникам, типам событий реализации риска ИБ и типам потерь, вследствие реализации риска ИБ, в соответствии с приложением 2 к настоящему Положению.

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

определение политики ИБ;

организацию ресурсного обеспечения (кадрового и финансового);

реализацию программ по обучению и повышению осведомленности в области противодействия угрозам безопасности информации;

реализацию взаимодействия с клиентами кредитной организации, в том числе в случае получения уведомлений об осуществлении переводов денежных средств без согласия клиентов;

обеспечение соответствия фактических значений контрольных показателей уровня риска ИБ, принятым в кредитной организации значениям;

планирование, реализация, контроль и совершенствование системы мер, направленных на повышение эффективности управления риском ИБ и снижение негативного влияния риска ИБ;

разработку стратегии обеспечения информационной безопасности;

распределение ролей и обязанностей, исключающее конфликт интересов в рамках организационной структуры обеспечения информационной безопасности;

должностное лицо (лицо, его замещающее), ответственное за функционирование системы информационной безопасности (с прямым подчинением единоличному исполнительному органу кредитной организации или его заместителю, а также не участвующее в совершении банковских операций, сделок, организации бухгалтерского и управленческого учета), обеспечение функционирования информационных систем;

критерии оценки эффективности службы информационной безопасности;

требования к квалификации работников, в том числе должностного лица, ответственного за функционирование системы информационной безопасности (с прямым подчинением руководителю единоличного исполнительного органа кредитной организации или его заместителю) и руководителя подразделения, выполняющего 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 управления риском ИБ, в том числе при передаче внешним контрагентам выполнения функций кредитной организации (головной кредитной организации банковской группы) и (или) использовании внешних информационных систем в рамках реализации направлений деятельности (в разрезе составляющих их банковских процессов) кредитной организации (головной кредитной организации банковской группы);

процессы обеспечения защиты информации, в том числе в целях обеспечения непрерывности оказания услуг при реализации направлений деятельности (в разрезе составляющих их банковских процессов) кредитной организации (головной кредитной организации банковской группы);

процессы управления инцидентами защиты информации и повышения ситуационной осведомленности об актуальных угрозах безопасности информации;

процессы реализации технологии обработки информации, подготавливаемой, обрабатываемой и хранимой при реализации направлений деятельности (в разрезе составляющих их банковских процессов) кредитной организации (головной кредитной организации банковской группы), в целях обеспечения целостности и достоверности указанной информации, а также протоколирования (журналирования) действий, совершаемых на этапах подготовки, обработки и хранения, в отношении нее;

процессы применения прикладного программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия не декларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия (далее – ОУД) не ниже чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014);

требования к информационным системам и другим техническим средствам обеспечения информационной безопасности, а также их классификацию по уровням соответствия требованиям;

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

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

независимую оценку на соответствие требованиям обеспечения информационной безопасности, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2017), ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 года № 423-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2014), проводимую кредитной организацией и (или) приглашенным квалифицированным экспертом.

7.8. Кредитная организация (головная кредитная организация банковской группы) в рамках реализации системы обеспечения информационной безопасности разрабатывает и обеспечивает соблюдение политики информационной безопасности, в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 24 сентября 2012 года № 423-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2014), включающую в том числе:

определение ролей и ответственности органов управления;

способы обеспечения информационной безопасности и защиты данных, а также порядок их применения;

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

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

требования по обмену информации о событиях риска ИБ, в том числе инцидентах защиты информации и предоставлению данных в Банк России, в соответствии с требованиями настоящего Положения;

показатели оценки эффективности реализации политики ИБ, сигнальные и контрольные значения контрольных показателей;

методики оценки эффективности обеспечения информационной безопасности и управления риском ИБ.

Политика информационной безопасности утверждается коллегиальным исполнительным органом кредитной организации.

Коллегиальный исполнительный орган кредитной организации несет ответственность в целом за соблюдение требований политики информационной безопасности и настоящего Положения.

7.9. Служба информационной безопасности в целях управления риском ИБ осуществляет следующие функции:

разработка политики информационной безопасности;

контроль соблюдения работниками кредитной организации мер обеспечения информационной безопасности и защиты информации и выполнение других задач, возложенных на него документами кредитной организации;

выявление, учет событий риска ИБ, мониторинг риска ИБ, в соответствии с требованиями главы 3 настоящего Положения, в том числе на

основе информации, предоставляемой другими центрами компетенций, ответственными за сбор информации о событиях операционного риска;

осуществление ведения базы событий риска ИБ;

участие в реализации процессов в рамках системы мер, направленных на повышение эффективности управления риском ИБ и снижение негативного влияния риска ИБ;

осуществление планирования и контроля процессов в рамках системы мер, направленных на повышение эффективности управления риском ИБ и снижение негативного влияния риска ИБ;

разработка предложений по совершенствованию процессов в рамках системы мер, направленных на повышение эффективности управления риском ИБ и снижения негативного влияния риска ИБ;

регистрация событий риска ИБ в базе событий;

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 кредитной организации;

осуществление мониторинга соблюдения значений лимитных показателей уровня риска ИБ, определенных в соответствии с пунктом 2 приложения 4 к настоящему Положению;

мониторинг эффективности управления риском ИБ;

направление информации о событиях риска ИБ в Банк России в соответствии с нормативным актом Банка России;

участие в разработке документов по управлению риском ИБ;

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

осуществление других функций, связанных с обеспечением информационной безопасности и управлением риском ИБ, предусмотренных документами кредитной организации.

7.10. Служба информационной безопасности формирует специализированную отчетность по рискам ИБ, направляемую на рассмотрение коллегиальному исполнительному органу кредитной организации, в дополнение к отчетности, формируемой подразделением, ответственным за организацию управления операционным риском, в соответствии с пунктом 4.2 настоящего Положения:

отчеты, в соответствии с требованиями Положения Банка России от 9 июня 2012 года № 382-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств», зарегистрированного Министерством юстиции Российской Федерации 14 июня 2012 года № 24575, 1 июля 2013 года № 28930, 10 сентября 2014 года № 34017, 22 июня 2018 года № 51411 (далее – Положение Банка России № 382-П);

сводные отчеты должностному лицу, ответственному за обеспечение информационной безопасности и коллегиальному исполнительному органу кредитной организации.

Кредитная организация (головная кредитная организация банковской группы) устанавливает порядок и сроки предоставления данной отчетности.

7.11. Уполномоченное подразделение проводит регулярную (не реже одного раза в год) независимую оценку требований, установленных настоящей главой Положения, в рамках оценки эффективности системы управления операционным риском.

Глава 8. **Требования к управлению риском информационных систем**

8.1. Кредитная организация (головная кредитная организация банковской группы) определяет систему управления риском ИС, как риском отказов и (или) нарушения (изменения) функционирования применяемых кредитной организацией (головной кредитной организацией банковской группы) информационных систем и (или) несоответствия их функциональных возможностей (характеристик) потребностям кредитной организации, включающую мероприятия и процедуры по обеспечению требований к непрерывности, безопасности, качеству функционирования информационных систем и обеспечению качества данных в информационных системах, 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» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736), требованиями национального стандарта Российской Федерации ГОСТ Р 53647.1-2009 «Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 15 декабря 2009 года № 998-ст «Об утверждении национальных стандартов» (М., ФГУП «Стандартинформ», 2009), ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года № 822-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2017), ГОСТ 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 1 июня 2016 года № 458-ст «Об утверждении национального стандарта» (М., Стандартинформ, 2016), 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; № 52, ст. 7491; 2017, № 18, ст. 2664; № 24, ст. 3478; № 25, ст. 3596; № 27, ст. 3953; № 31, ст. 4790, 4825, 4827; № 48, ст. 7051; 2018, № 1 , ст. 66; № 18, ст. 2572; № 27, ст. 3956; № 30, ст. 4546; № 52, ст. 8101).

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

8.3. Коллегиальный исполнительный орган кредитной организации обеспечивает соблюдение и определяет в Политике информационных систем:

роли и ответственность структурных подразделений по исполнению Политики информационных систем и требований настоящей главы Положения;

должностное лицо (лицо, его замещающее), ответственное за обеспечение функционирования информационных систем кредитной организации (далее – должностное лицо, ответственное за ИС) и координацию деятельности структурных подразделений кредитной организации, ответственных за функционирование ИС или ее компонентов;

перечень ИС, обеспечивающих функционирование банковских процессов;

требования к ИС, в том числе требования по обеспечению непрерывности, безопасности и качества функционирования ИС;

порядок информационного обмена в рамках реализации Политики информационных систем;

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

8.4. Должностное лицо (лицо, его замещающее), ответственное за ИС, проводит не реже одного раза в год анализ необходимости пересмотра требований Политики информационных систем в зависимости от характера и масштаба осуществляемых операций, действующих банковских процессов, изменяющихся факторов внешней среды и стратегии развития кредитной организации, результатов процедур управления операционным риском, результатов оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением и выносит результаты анализа на рассмотрение коллегиальным исполнительным органом кредитной организации для принятия решения о необходимости изменений Политики информационных систем и документов.

Кредитная организация (головная кредитная организация банковской группы) определяет в документах порядок и правила проведения анализа и пересмотра Политики информационных систем.

8.5. Кредитная организация (головная кредитная организация банковской группы) идентифицирует и закрепляет в Политике информационных систем перечень ИС, обеспечивающих функционирование банковских процессов, в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, в том числе, требующих обеспечения

информационного обмена, обработки, хранения и защиты информации посредством реализации ИС.

8.6. Кредитная организация (головная кредитная организация банковской группы) обеспечивает проведение структурными подразделениями кредитной организации в соответствии с требованиями абзаца 3 пункта 8.3 настоящего Положения мероприятий, направленных на выявление, оценку, разработку форм (способов) контроля и мер, направленных на повышение качества системы управления риском ИС и снижение негативного влияния риска ИС и сопряженных с ним рисков ИБ, влияющих на ИС (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 обеспечение функционирования и бесперебойной работы банковских процессов кредитной организации, включающие:

8.7.1. Требования к структуре ИС:

состав основных функций, компонентов, подсистем ИС, и их иерархической структуры в соответствии с заданными функциональными требованиями и техническими заданиями и с учетом требований стандарта ГОСТ 34.601-90 «Государственный стандарт союза ССР. Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания», утвержденного Постановлением Государственного комитета СССР по управлению качеством продукции и стандартам от 29 декабря 1990 года № 3469 (М., ИПК Издательство стандартов, 1997), ГОСТ 34.602-89 «Межгосударственный стандарт. Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание

автоматизированной системы», утвержденного Постановлением Госстандарта СССР от 24 марта 1989 года № 661 (М., ИПК Издательство стандартов, 2004);

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 других 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 рабочей документации;

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

квалификацию и сертификацию работников, задействованных 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 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 примерные варианты решения, а также требования к информационному, техническому и программному обеспечению ИС;

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

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

перечень показателей надежности функционирования ИС и их пороговые значения;

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

меры по повышению качества функционирования ИС;

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

другие требования, отражающие особенности обеспечения функционирования банковских процессов и структуры ИС кредитной организации.

8.7.4. Требования к обеспечению качества данных в ИС в разрезе характеристик качества данных, включая:

точность и достоверность данных, в части отсутствия синтаксических и семантических ошибок в данных, а также их соответствия реальным и

статистически наиболее вероятным значениям свойств, характеристик и параметров, зафиксированных в данных;

полноту данных, в части достаточности объема данных (количества хранящихся в ИС записей), глубины данных (периода данных, используемого для проведения операций и оценки эффективности банковских процессов, применяемых методик и моделей банковских процессов) и широты данных (охвата данными всех разрезов, свойств и характеристик объектов), требуемых в рамках обеспечения функционирования банковских процессов;

актуальность данных, как свойство данных в любой момент времени адекватно отражать состояние объектов предметной области;

согласованность данных, как взаимная непротиворечивость данных, хранящихся в ИС банка, других источниках и носителях информации, унификация данных при их перемещении в ИС и банковских процессах, целостность соответствующих идентификационных ссылок и связей в структурах баз данных;

доступность данных, как возможность использования данных для обеспечения функционирования банковских процессов;

контролируемость данных, как возможность осуществления контроля качества и происхождения данных, в том числе посредством отражения в ИС источников данных, истории создания, изменения, преобразования, удаления, хранения и передачи данных;

восстанавливаемость данных, как возможность сохранять установленный уровень функциональности и качества данных после их утраты, повреждения или изменения в результате сбоев или других нарушений функционирования ИС;

другие характеристики качества данных, определяемые кредитной организацией в документах кредитной организации.

Кредитная организация (головная кредитная организация банковской группы) с учетом характера и масштаба осуществляемых операций, уровня и сочетания принимаемых рисков, действующих банковских процессов,

текущих и стратегических планов развития и доступных возможностей определяет в документах дополнительные характеристики качества и другие требования к качеству данных в ИС, включающие разработку методики обеспечения качества данных и порядка обеспечения качества данных.

8.7.4.1 Методику обеспечения качества данных в ИС, обеспечивающих критически важные процессы, включающую следующие элементы:

классификатор возможных источников и причин образования некачественных данных в ИС;

показатели (индикаторы) качества данных для оценки характеристик, разрабатываемые кредитной организацией для различных ИС, использующих данные;

методы и алгоритмы расчета, правила измерения показателей качества данных, в том числе с использованием контрольных выборок данных;

критерии оценки качества данных.

Кредитная организация (головная кредитная организация банковской группы) определяет в документах другие элементы методики обеспечения качества данных в ИС.

Указанные элементы разрабатываются и применяются с учетом особенностей конкретных данных, в том числе методов и процедур их фиксирования, хранения и преобразования, а также типов и форматов.

8.7.4.2. Порядок обеспечения качества данных в ИС, обеспечивающих критически важные процессы, включающий следующие элементы:

процедуры измерения показателей качества данных;

процедуры обоснования, утверждения и корректировки предельно допустимых значений показателей качества данных, критериев оценки качества данных;

процедуры реагирования на случаи нарушения установленных кредитной организацией (головной кредитной организацией банковской группы) предельно допустимых значений показателей качества данных, установленных критериев оценки качества данных;

процедуры, правила и периодичность контроля и формирования отчетов о качестве данных, о соблюдении мер контроля качества данных;

процедуры исправления выявленных ошибок в данных и документирования внесенных изменений;

порядок взаимодействия по вопросам обеспечения качества данных органов управления, подразделений и должностных лиц кредитной организации, устанавливающий их полномочия, ответственность, подотчетность и обеспечение ресурсами, в том числе определение в кредитной организации должностного лица (лиц), несущего (несущих) персональную ответственность за обеспечение требуемого качества данных в ИС;

порядок и периодичность (не реже одного раза в год) проведения независимой оценки качества данных.

Кредитная организация определяет в документах другие элементы порядка обеспечения качества данных в ИС.

8.7.5. Кредитная организация (головная кредитная организация банковской группы) определяет в документах дополнительные требования к ИС и их функционированию с учетом характера и масштаба осуществляемых операций, уровня и сочетания принимаемых рисков, действующих банковских процессов, текущих и стратегических планов развития и доступных возможностей.

8.7.6. Подразделение, ответственное за функционирование ИС, не реже одного раза в год проводит анализ необходимости пересмотра требований к ИС с учетом текущих и стратегических планов развития, их влияния на банковские процессы, а также оценки уровня операционного риска, отраженной в отчетности по операционному риску и мер, направленных на повышение качества системы операционным риском и снижение негативного влияния операционного риска, отчетов службы информационной безопасности и подразделения, ответственного за обеспечение информационной безопасности и подразделения, ответственного за работу ИС, и направляет результаты анализа коллегиальному исполнительному

органу кредитной организации для принятия решения о пересмотре требований к ИС.

8.8. Кредитная организация (головная кредитная организация банковской группы) разрабатывает, соблюдает и отражает в 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 части управления рисками ИБ, в соответствии с главой 7 настоящего Положения.

8.8.2 Обеспечение технических условий эксплуатации технических средств элементов ИС, а также устройств бесперебойного электропитания, пожаротушения, вентиляции и кондиционирования, резервных цифровых каналов и устройств связи, резервных носителей данных.

8.8.3 Регулярное (не реже одного раза в день) резервное копирование данных критически важных банковских процессов на резервные технические средства, размещенные в других 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 подпункта 8.8.2 настоящего пункта Положения, режим охраны и доступа.

8.8.4 Использование лицензионного и сертифицированного программного обеспечения, то есть принятого в эксплуатацию с соблюдением требований подпункта 8.7.2 пункта 8.7 настоящего Положения, с соблюдением технических условий эксплуатации, описанных в эксплуатационной документации программного обеспечения.

8.8.5. Наличие в документах кредитной организации положения и стратегии по обеспечению непрерывности и восстановления функционирования ИС. Кредитная организация (головная кредитная организация банковской группы) определяет коллегиальный исполнительный орган кредитной организации по утверждению положения и стратегии по

обеспечению непрерывности и восстановления функционирования ИС, с установлением обязательств соблюдения требований указанных документов всеми структурными подразделениями кредитной организации (головной кредитной организация банковской группы), в части их касающейся.

8.8.6. Проведение кредитной организацией регулярных (не реже одного раза в год) оценок состава компонентов, архитектуры, инфраструктуры и характеристик ИС на предмет их достаточности и эффективности для обеспечения функционирования банковских процессов кредитной организации, по результатам которых принимаются меры по устранению выявленных недостатков в ИС.

8.8.7. Ежегодное тестирование недостатков ИС или их компонентов и других источников риска ИС, в том числе разработку системы мер, направленных на устранение выявленных недостатков ИС и (или) других источников риска ИС.

8.8.8. Проведение уполномоченным подразделением регулярной (не реже одного раза в год) независимой оценки соблюдения установленных настоящей главой Положения требований, включающих оценку эффективности:

соблюдения Политики ИС;

мероприятий, направленных на выявление, регулирование, разработку мер, направленных на повышение качества системы управления риском ИС и снижение негативного влияния 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 соблюдения требований, установленных настоящей главой Положения, коллегиальному исполнительному органу кредитной

организации, подразделениям, ответственным за обеспечение функционирования ИС и службе управления рисками.

8.8.9. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) определяет подразделение (одно или несколько), ответственное за обеспечение непрерывности функционирования ИС, включая:

определение полномочий подразделения и его работников;

целевые показатели и критерии эффективности работы подразделения, с занесением их в положение о подразделении и должностные инструкции работников;

контрольные процедуры и целевые показатели, включая порядок их актуализации;

8.8.10. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) определяет должностное лицо (лицо, его замещающее), ответственное за обеспечение непрерывности функционирования ИС в кредитной организации, включая его полномочия и требования к его квалификации и сертификации;

8.8.11. Должностное лицо (лицо, его замещающее), ответственное за обеспечение непрерывности функционирования ИС в кредитной организации, регулярно (не реже одного раза в год) проводит самооценку рисков ИС в разрезе банковских процессов и соблюдения требований настоящей главы и направляет отчеты по результатам самооценки в подразделение, ответственное за организацию управления операционным риском, и (или) другому уполномоченному органу.

8.8.12. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) определяет подразделение, ответственное за предоставление отчетности по риску ИС, в соответствии с требованиями подпункта 4.2.1 пункта 4.2 настоящего Положения, а также порядок предоставления отчетности подразделению, ответственному за организацию управления операционным риском.

8.8.13. Кредитная организация (головная кредитная организация банковской группы) определяет в документах дополнительные требования к обеспечению постоянного функционирования ИС, безопасности и качеству функционирования ИС с учетом характера и масштаба осуществляемых операций, принимаемых рисков, действующих банковских процессов, текущих и стратегических планов развития и доступных возможностей.

Глава 9. **Особенности применения требований настоящего Положения кредитными организациями в зависимости от характера и масштаба деятельности**

9.1 Особенности применения требований настоящего Положения различаются для следующих категорий кредитных организаций:

банк с универсальной лицензией, размер активов которого составляет 500 миллиардов рублей на начало текущего отчетного года в соответствии со значением показателя «Всего активов» в строке 12 формы 0409806 «Бухгалтерский баланс (публикуемая форма)», установленной приложением 1 к Указанию Банка России от 8 октября 2018 года № 4927-У «О перечне, формах и порядке составления и представления форм отчетности кредитных организаций в Центральный банк Российской Федерации», зарегистрированному Министерством юстиции Российской Федерации 13 декабря 2018 года № 52992 (далее – Указание Банка России № 4927-У), (далее – крупный банк);

банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей на начало текущего отчетного года в соответствии со значением показателя «Всего активов» в строке 12 формы 0409806 «Бухгалтерский баланс (публикуемая форма)», установленной приложением 1 к Указанию Банка России № 4927-У (далее – банк с универсальной лицензией, не признаваемый крупным);

банк с базовой лицензией и небанковская кредитная организация, за исключением центрального контрагента (далее – банк с базовой лицензией и НКО).

Отнесение банка к определенной категории для целей соблюдения требований настоящего Положения действует до конца отчетного года и не изменяется в течение отчетного года.

9.2. Крупный банк обеспечивает соблюдение всех требований настоящего Положения с учетом особенностей переходного положения, установленными в пунктах 10.2-10.5 настоящего Положения, в том числе:

Крупный банк в соответствии с пунктом 3.12 настоящего Положения применяет следующие процедуры и способы, указанные в подпунктах 3.2.1, 3.2.2, 3.2.3 пункта 3.2, подпунктах 3.6.1, 3.6.4, 3.6.5, 3.6.7 пункта 3.6 настоящего Положения, в дополнение к другим способам, определенным кредитной организацией.

9.3. Банк с универсальной лицензией, не признаваемый крупным, обязан соблюдать все требования настоящего Положения с учетом следующих особенностей:

9.3.1 Банк с универсальной лицензией, не признаваемый крупным, обеспечивает выполнение пунктов 1.1, 1.4, 1.5 настоящего Положения, в том числе:

в части выполнения требований, установленных пунктом 1.2 настоящего Положения, с учетом порога регистрации, регистрирует в базе событий события операционного риска с прямыми и (или) косвенными потерями, потерями клиентов и третьих лиц;

в части выполнения требований, установленных абзацем 7 пункта 1.3 настоящего Положения, в случае отсутствия в организационно-штатной структуре подразделения, ответственного за организацию управления операционным риском, назначает работника без совмещения должностных обязанностей с организацией управления другими рисками;

9.3.2. Банк с универсальной лицензией, не признаваемый крупным, обеспечивает выполнение требований главы 2 настоящего Положения с учетом требований абзаца 2 подпункта 9.3.1 пункта 9.3 настоящего Положения.

9.3.3. Банк с универсальной лицензией, не признаваемый крупным, обеспечивает выполнение требований главы 3 настоящего Положения и применяет процедуры и способы, предусмотренные подпунктами 3.2.1, 3.2.2 пункта 3.2, пунктами 3.3, 3.4, подпунктами 3.5.1, 3.5.2 пункта 3.5, подпунктами 3.6.1, 3.6.5, 3.6.7 пункта 3.6 настоящего Положения (в случае если кредитная организация (головная кредитная организация банковской группы) использует, в соответствии с пунктом 5.1 Указания Банка России № 3624-У, методы оценки величины риска и общей потребности в капитале, отличные от установленных Банком России), 3.7 – 3.9 настоящего Положения.

9.3.4. Банк с универсальной лицензией, не признаваемый крупным, обеспечивает выполнение требований главы 4 настоящего Положения с учетом требований абзаца 2 подпункта 9.3.1 пункта 9.3 настоящего Положения и подпункта 9.3.3 пункта 9.3 настоящего Положения.

9.3.5. Банк с универсальной лицензией, не признаваемый крупным, обеспечивает выполнение требований глав 5-8 настоящего Положения с учетом требований абзаца 2 подпункта 9.3.1 пункта 9.3 настоящего Положения и пункта 9.3.3 настоящего Положения.

9.3.6. Банк с универсальной лицензией, не признаваемый крупным, в документах определяет перечень оставшихся требований настоящего Положения, которые будет дополнительно соблюдать исходя из характера и масштаба деятельности.

9.4. Банк с базовой лицензией и НКО обязаны соблюдать требования настоящего Положения с учетом следующих особенностей.

9.4.1 Банк с базовой лицензией и НКО обеспечивают выполнение пунктов 1.1, 1.4, 1.5 настоящего Положения, в том числе:

В части выполнения требований, установленных пунктом 1.2 настоящего Положения, регистрирует в базе событий события операционного риска с прямыми потерями, потерями клиентов;

В случае отсутствия возможности создания подразделения, ответственного за организацию управления операционным риском, банк с базовой лицензией и НКО, в части выполнения требований, установленных абзацем 6 пункта 1.3 настоящего Положения, назначает работника, ответственного за организацию управления операционным риском, с возможным совмещением должностных обязанностей с организацией управления другими рисками.

В случае отсутствия в организационно-штатной структуре специализированных подразделений, которые управляют отдельными видами операционного риска, банк с базовой лицензией и НКО, в части выполнения требований, установленных абзацем 7 пункта 1.3 настоящего Положения, назначает работников с возложением трудовых обязанностей по управлению отдельными видами риска, определенными в пункте 1.4 настоящего Положения.

9.4.2. Банк с базовой лицензией и НКО обеспечивают выполнение требований главы 2 настоящего Положения с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения.

9.4.3. Банк с базовой лицензией и НКО обеспечивают выполнение требований главы 3 настоящего Положения и применяет процедуры и способы, предусмотренные подпунктом 3.2.1 пункта 3.2, пунктами 3.3 (за исключением подпункта 3.3.1), 3.4, подпунктом 3.5.1 пункта 3.5 настоящего Положения, с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения.

В части выполнения требований, установленных пунктом 3.7 настоящего Положения, банк с базовой лицензией и НКО обеспечивают выбор и применение способа реагирования, в том числе принятие мер, направленных на повышение качества системы управления операционным риском и

снижение негативного влияния операционного риска только в части реализовавшихся событий операционного риска с прямыми потерями.

Требования, установленные в пунктах 3.8 и 3.9 настоящего Положения, на банки с базовой лицензией и НКО, не распространяются.

9.4.4. Банк с базовой лицензией и НКО обеспечивают выполнение требований главы 4 настоящего Положения с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения и подпункта 9.4.3 пункта 9.4 настоящего Положения.

9.4.5. Банк с базовой лицензией и НКО обеспечивают выполнение требований глав 5-6 настоящего Положения с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения и подпункта 9.4.3 пункта 9.4 настоящего Положения.

9.4.6. Банк с базовой лицензией и НКО обеспечивают выполнение требований главы 7 настоящего Положения с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения и подпункта 9.4.3 пункта 9.4 настоящего Положения.

9.4.7. Банк с базовой лицензией и НКО обеспечивают выполнение требований главы 8 настоящего Положения с учетом требований абзаца 2 подпункта 9.4.1 пункта 9.4 настоящего Положения и подпункта 9.4.3 пункта 9.4 настоящего Положения, в том числе:

в части выполнения требований, установленных пунктом 8.6 настоящего Положения обеспечивают выявление риска ИБ;

обеспечивают выполнение абзацев 7 и 8 подпункта 8.7.2 пункта 8.7 настоящего Положения;

обеспечивают выполнение абзацев 1, 3, 4 подпункта 8.7.3 пункта 8.7 настоящего Положения;

обеспечивают выполнение абзацев 1-8 подпункта 8.7.4 пункта 8.7 настоящего Положения;

обеспечивают выполнение абзаца 1 подпункта 8.8.9 пункта 8.8 настоящего Положения.

Требования, установленные в подпунктах 8.8.6, 8.8.7 и 8.8.11 пункта 8.8 настоящего Положения, на банки с базовой лицензией и НКО не распространяются.

9.4.8. Банк с базовой лицензией и НКО определяют в документах перечень требований настоящего Положения, который банк с базовой лицензией и НКО дополнительно применяют исходя из масштабов и характера совершаемых операций, уровня и объемов операционного риска.

Глава 10. **Заключительные положения**

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

10.2. Крупным банкам (головным кредитным организациям банковской группы) привести систему управления операционным риском в соответствие с настоящим Положением в срок до 31 декабря 2019 года.

10.3. Банкам с универсальной лицензией (головным кредитным организациям банковской группы), не признаваемым крупными, привести систему управления операционным риском в соответствие с настоящим Положением в срок до 31 декабря 2020 года.

10.4. Банкам с базовой лицензией и НКО привести систему управления операционным риском в соответствие с настоящим Положением в срок до 31 декабря 2021 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 «неразрешенные действия персонала», включающий:

1.1. Неразрешенная деятельность, состоящая в преднамеренных действиях работников, связанная с превышением работниками своих полномочий при проведении или одобрении сделки (осуществлении операций), закрепленных должностными инструкциями, документами или решениями единоличного или коллегиального исполнительных органов кредитной организации, без цели присвоения имущества, материальных и (или) нематериальных активов, но в целях получения другой нематериальной выгоды.

1.2. Противоправные действия 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 том числе с использованием коммерческого подкупа (коррупции).

2. Тип события «преднамеренные действия третьих лиц», включающий:

2.1. Противоправные действия 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 кибератак, совершенных третьими лицами с применением средств цифровой инфраструктуры (реализации событий киберриска) по отношению к информации и данным, содержащимся во внутренних ИС банка;

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

3.1. Нарушение трудового законодательства, результатом которого стало наложение на кредитную организацию санкций за нарушение норм трудового законодательства (например, выплаты работникам (или бывшим работниками) и (или) дисквалификация работников (или бывших работников) в виде компенсаций за нарушение условий трудового договора и (или) наложение федеральным органом исполнительной власти, уполномоченным на осуществление федерального государственного надзора за соблюдением трудового законодательства).

3.2. Нарушение государственных нормативных требований охраны труда, состоящее в нарушении кредитной организацией норм безопасности и охраны труда, в том числе действие (бездействие) должностных лиц по соблюдению 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 и по возрастному признаку).

4. Тип события «нарушения прав клиентов и контрагентов, включая нанесение им ущерба», включающий:

4.1. Нарушения прав клиентов, состоящие в действиях со стороны кредитной организации, которые привели к несанкционированному раскрытию конфиденциальной информации, нарушению функционирования системы информационного обмена и взаимодействия с клиентом, повлекшие выплаты клиентам в связи с нарушением их интересов.

4.2. Нарушение обычаев делового оборота и рыночных практик, состоящее в нарушении кредитной организацией законодательства Российской Федерации и других государств, под юрисдикции которых попадают совершаемые операции, условий договоров на совершение банковских операций, стандартов поведения профессионального участника 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 организацией интересов и прав клиентов вследствие установленных в кредитной организации правил и стандартов оказания услуг и проведения операций, рекламы кредитной организации, навязывания сопутствующих услуг. К данному типу событий не относятся события, произошедшие в результате недостатка банковских процессов.

4.4. Нарушение требований законодательства в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

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) и нематериальным активам», включающие события стихийного характера и прочие внешние факторы, повлекшие досрочное списание (полное или частичное выбытие) материальных и (или) нематериальных активов кредитной организации:

5.1. Природные катастрофы.

5.2. Техногенные катастрофы.

5.3. Социальные катастрофы.

5.4. Медико-биологические катастрофы.

5.5. Вандализм.

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 других 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, оказавших влияние на деятельность кредитной организации.

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 процессов, 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 неразрешенными действиями персонала), события, связанные с несовершенством (недостатками) внутренних процессов, системы

внутреннего контроля, управления рисками, недостатков распределения ролей и полномочий, ошибками 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 другой 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 нарушении 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.

7.7. Нарушения правил и процедур противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, и финансированию распространения оружия массового уничтожения.

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 настоящего Положения и трех видов нарушения защиты информации:

1.1. События киберриска, связанные с переводами денежных средств и приводящие к следующим последствиям:

использование электронных средств платежа клиентов кредитных организаций без их согласия;

несанкционированный доступ к объектам информационной инфраструктуры кредитной организации, приведшие к несанкционированным переводам и снятиям денежных средств;

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

неоказание кредитной организацией услуг по переводу денежных средств;

выявление оператором по переводу денежных средств, включая оператора электронных денежных средств, и (или) оператором услуг платежной инфраструктуры атак, последствия от реализации которых приводят к случаям и попыткам осуществления переводов денежных средств без согласия клиента;

выявление кредитной организацией компьютерных атак, последствия от реализации которых приводят к случаям и попыткам осуществления банковской операции без согласия клиента;

неоказание услуг оператора по переводу денежных средств на период более 2 часов в целом по всем субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания;

неоказание услуг оператора по переводу денежных средств на период более 2 часов в целом в разрезе субъектов Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием платежных карт, их реквизитов и (или) систем (средств) дистанционного банковского обслуживания;

неоказание оператором по переводу денежных средств услуг по переводу денежных средств;

другие 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», 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;

неоказание или несвоевременное оказание банковских услуг;

выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций по переводу денежных средств и получению наличных денежных средств, совершенных в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, в том числе при уменьшении остатка электронных денежных средств, за исключением виртуальных платежных карт;

выполнение банковских операций в результате несанкционированного доступа к объектам информационной инфраструктуры кредитной организации;

осуществление несанкционированного снятия денежных средств оператора по переводу денежных средств в банкоматах;

осуществление несанкционированного снятия денежных средств оператора электронных денежных средств в банкоматах;

другие 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 потере конфиденциальной информации кредитной организации;

копированию конфиденциальных данных работниками кредитной организации;

хищению или утрате носителей информации кредитной организации;

неоказанию расчетным центром расчетных услуг на период более одного операционного дня;

невыполнению расчетным центром в течение операционного дня расчетов для принятых к исполнению распоряжений платежного клирингового центра или участников платежной системы;

прерыванию клиринговым центром предоставления услуг платежного клиринга на период более одного операционного дня;

невыполнению клиринговым центром в течение операционного дня платежного клиринга для принятых к исполнению распоряжений участников платежной системы;

прерыванию операционным центром предоставления операционных услуг на период более 2 часов;

другим нарушениям.

2. Риск ИБ дополнительно классифицируется 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 подпунктом 2.3.1 пункта 2.3 настоящего Положения:

ошибки и недостатки процессов применения кредитными организациями технологических мер, направленных на обеспечение целостности и достоверности информации, обрабатываемой на технологических участках направлений деятельности (в том числе в разрезе составляющих их банковских процессов) кредитной организации, в том числе

мер, направленных на протоколирование действий по обработке информации на указанных технологических участках;

ошибки и недостатки процессов применения программного обеспечения автоматизированных систем и приложений, сертифицированных в системе сертификации Федеральной службы по техническому и экспортному контролю на соответствие требованиям по безопасности информации, включая требования по анализу уязвимостей и контролю отсутствия недекларированных возможностей, в соответствии с законодательством Российской Федерации или в отношении которых проведен анализ уязвимостей по требованиям к оценочному уровню доверия не ниже ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст «Об утверждении национального стандарта» (М., ФГУП «Стандартинформ», 2014);

ошибки и недостатки процессов применения мер, направленных на повышение эффективности управления риском ИБ и снижение негативного влияния риска ИБ;

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», зарегистрированным Министерством юстиции Российской Федерации 6 декабря 2016 года № 44582 (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);

другие недостатки внутренних процессов, обеспечивающих функционирование информационной инфраструктуры кредитной организации и систем защиты информации.

2.2 По категории источников риска в соответствии с подпунктом 2.3.2 пункта 2.3 настоящего Положения:

реализация несанкционированного доступа персонала кредитной организации или третьих лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры кредитной организации (далее – действия внутреннего нарушителя);

реализация компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры участника кредитной организации (далее – действия внешнего нарушителя);

совместные и (или) согласованные действия внешнего и внутреннего нарушителя.

2.3. По категории источников риска в соответствии с подпунктом 2.3.3 пункта 2.3 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 подпунктом 2.3.4 пункта 2.3 настоящего Положения:

воздействия со стороны третьих лиц или информационных систем с целью блокирования штатного функционирования банковских 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 других 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 настоящего приложения, в зависимости от процессов кредитной организации, в которых они произошли.

2.6. В рамках дополнительной детализации классификации источников риска ИБ кредитные организации классифицируют источники (причины)риска реализации информационных угроз, в разрезе направлений компьютерных атак, типов компьютерных атак и типов атакуемых объектов:

2.6.1. По направлению компьютерных атак:

направленные на инфраструктуру кредитной организации;

направленные на клиента кредитной организации.

2.6.2. По типам компьютерных атак:

компьютерные атаки, связанные с изменением маршрутно-адресной информации;

компьютерные атаки, связанные с использованием вредоносного программного обеспечения применительно к объектам информационной инфраструктуры кредитных организаций и их клиентов;

компьютерные атаки, возникшие в результате побуждения клиентов к осуществлению операций по переводу денежных средств путем обмана или злоупотребления доверием;

компьютерные атаки типа «отказ в обслуживании» применительно к информационной инфраструктуре кредитной организации;

компьютерные атаки, связанные с реализацией несанкционированного доступа к банкоматам и платежным терминалам кредитных организаций;

компьютерные атаки, связанные с эксплуатацией уязвимостей информационной инфраструктуры кредитных организаций и их клиентов;

компьютерные атаки, связанные с подбором (взломом), компрометацией аутентификационных (учетных) данных;

компьютерные атаки, связанные с реализацией спам-рассылки, осуществляемой в отношении кредитных организаций и их клиентов;

компьютерные атаки, связанные с выявлением взаимодействия объектов информационной инфраструктуры кредитных организаций с командными центрами «Ботнет»;

компьютерные атаки, связанные с изменением (подменой) идентификатора мобильного абонента номера идентификационного модуля абонента, а также с заменой идентификатора мобильного оборудования;

компьютерные атаки, связанные с информацией, вводящей работников кредитных организаций и их клиентов, а также третьих лиц, взаимодействующих с ними, в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания;

компьютерные атаки, связанные с распространением информации, касающейся предложения и (или) предоставления на территории Российской Федерации финансовых услуг лицами, не имеющими права их оказывать в соответствии с законодательством Российской Федерации (размещение в сети Интернет запрещенного контента);

компьютерные атаки, связанные с размещением в сети Интернет информации, позволяющей осуществить неправомерный доступ к информационным системам кредитных организаций и их клиентов, используемым для выполнения банковских и (или) технологических процессов при оказании (получении) банковских услуг, в том числе путем неправомерного доступа к конфиденциальной информации клиентов (размещение в сети Интернет вредоносного ресурса);

компьютерные атаки, связанные с изменением контента;

компьютерные атаки, связанные со сканированием программных портов объектов информационной инфраструктуры кредитных организаций лицами, не обладающими соответствующими полномочиями;

другие компьютерные атаки, направленные на объекты информационной инфраструктуры кредитных организаций и их клиентов.

2.6.3. По типам атакуемых объектов:

2.6.3.1. На системном уровне информационной инфраструктуры:

аппаратное обеспечение;

сетевое оборудование;

сетевые приложения и сервисы;

серверные компоненты виртуализации, программные инфраструктурные сервисы;

операционные системы, системы управления базами данных, сервера приложений.

2.6.3.2. На уровне автоматизированных систем и приложений, используемых для выполнения банковских и (или) технологических процессов кредитной организации при оказании банковских услуг:

система дистанционного банковского обслуживания;

система обработки транзакций, осуществляемых с использованием платежных карт;

информационный ресурс сети Интернет;

автоматизированная банковская система;

система посттранзакционного обслуживания операций, осуществляемых с использованием платежных карт;

автоматизированная система, используемая персоналом кредитной организации.

2.6.3.3. На уровне автоматизированных систем и приложений, используемых клиентом кредитной организации при получении банковских услуг:

файловый сервер;

система дистанционного банковского обслуживания;

сервер электронной почты;

автоматизированная система, используемая персоналом кредитной организации.

2.6.3.4. Другой тип системы.

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

3. В рамках дополнительной детализации классификации риска ИБ в разрезе направлений деятельности (в том числе в разрезе составляющих их банковских процессов) кредитные организации классифицируют направления деятельности (в том числе в разрезе составляющих их банковских процессов) по способам формирования и передачи распоряжений на осуществление транзакций, позволяющим совершить банковскую операцию при:

использовании технологии дистанционного обслуживания, при которой обмен информацией между кредитной организацией и ее клиентом

осуществляется с применением коротких текстовых сообщений с определенного в договоре банковского счета номера телефона;

использовании технологии дистанционного обслуживания, при которой обмен информацией между кредитной организацией и ее клиентом осуществляется с применением программного обеспечения, разрабатываемого для использования в операционных системах мобильных устройств;

использовании технологии дистанционного обслуживания, при которой обмен информацией между кредитной организацией и ее клиентом осуществляется с применением интернет-браузера без установки дополнительного программного обеспечения;

использовании технологии дистанционного обслуживания, при которой обмен информацией между кредитной организацией и ее клиентом осуществляется с персонального компьютера с применением дополнительного программного обеспечения, предоставляемого кредитной организацией;

использовании банкомата;

использовании банкомата с возможностью приема наличных денежных средств;

использовании банкомата с функцией ресайклинга;

использовании электронного программно-технического устройства для приема к оплате платежных карт;

использовании платежного терминала;

осуществлении переводов с использованием платежных карт без непосредственного использования платежных карт;

другом способе формирования и передачи распоряжений на осуществление транзакций, позволяющем совершить банковскую операцию.

4. 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.

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

потери денежных средств или других активов кредитной организации, в результате реализации рисков ИБ, указанных в подпункте 1.1 пункта 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.

4.2. По категории «косвенные потери»:

расчетные потери из-за простоев информационной инфраструктуры или потери ее работоспособности в результате реализации рисков ИБ, указанных в подпункте 1.1 пункта 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.

4.3. По категории «качественные потери»:

простои банковских процессов;

потеря работоспособности информационной инфраструктуры;

нарушение целостности (искажение) или потеря данных;

возникновение уязвимостей в информационной инфраструктуре, программном обеспечении и приложениях, банковских процессах;

другие потери качества информационной инфраструктуры кредитной организации.

4.4. 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 повышение качества системы управления операционным риском и снижение негативного влияния операционного риска.

Кредитная организация использует, но не ограничивается следующим перечнем возможных мер, направленных на повышение качества системы управления операционным риском и снижение негативного влияния операционного риска.

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

1.2. Применение стандартизированных форм документов кредитной организации;

1.3. Стандартизация операций (сделок);

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

1.5. Контроль (автоматизированный, ручной) за соблюдением 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 банковских процессов, технологических, информационных систем кредитной организации;

1.14. Автоматизация банковских процессов (операций), алгоритмизация 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 банковских 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 банковских 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. Другие меры, направленные на уменьшение негативного влияния 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 в соответствии с главой 5 настоящего Положения.

1.1. Базовый набор показателей системы управления операционными рисками.

1.1.1. Для банков с базовой лицензией и НКО (участников банковской группы):

общая сумма валовых прямых потерь понесенных кредитной организации от реализации событий операционного риска за вычетом потерь от событий риска ИБ за определенный период (нарастающим 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 чистых прямых потерь за год (включая чистые прямые потери от событий риска ИБ), понесенных кредитной организацией за год, к показателю Д, рассчитанному в соответствии с пунктом 3 Положения Банка России № 652-П на последнюю отчетную дату;

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 пунктом 3 Положения Банка России № 652-П на последнюю отчетную дату;

отношение суммы чистых прямых потерь от реализации событий операционного риска (в соответствии с пунктом 6.18 настоящего Положения) за вычетом потерь от событий риска ИБ, к показателю Д, рассчитанному в соответствии с пунктом 3 Положения Банка России № 652-П на последнюю отчетную дату;

доля выявленных в ходе оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, внешним экспертом, или Банком России событий операционного риска с прямыми потерями, превышающими порог регистрации (за исключением потерь от кредитного риска) в соответствии с пунктом 6.5 настоящего Положения, которые кредитная организация не отразила в базе событий, по отношению ко всем зарегистрированным в базе событий событиям операционного риска с прямыми потерями (за исключением потерь от кредитного риска), превышающими порог регистрации (за исключением потерь от кредитного риска) в соответствии с пунктом 6.5 настоящего Положения, за годовой период, к которому относится проверяемый период (контрольное значение должно быть не больше 5%, сигнальное значение – не больше 3%);

отношение сумм валовых прямых потерь от выявленных в ходе оценки эффективности функционирования системы управления операционного риска, проведенной уполномоченным подразделением, внешним экспертом, или Банком России событий операционного риска с прямыми потерями, превышающими порог регистрации (за исключением потерь от кредитного риска) в соответствии с пунктом 6.5 настоящего Положения, которые кредитная организация не отразила в базе событий к общей сумме валовых прямых потерь всех зарегистрированных в базе событий с прямыми потерями (за исключением потерь от кредитного риска), превышающими порог регистрации (за исключением потерь от кредитного риска) в соответствии с

пунктом 6.5 настоящего Положения, за годовой период, к которому относится проверяемый период (контрольное значение должно быть не больше 5%, сигнальное значение – не больше 3%);

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

1.1.2. Крупные банки и банки с универсальной лицензией, не признаваемые крупными, кроме базовых показателей, перечисленных в подпункте 1.1.1 настоящего пункта приложения, используют следующие дополнительные показатели:

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

отношение чистых 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 относятся качественные оценки по четырехуровневой системе («хорошо», «удовлетворительно», «сомнительно», «неудовлетворительно») по следующим направлениям:

оценка эффективности функционирования системы управления операционным риском, проведенная уполномоченным подразделением, в соответствии с пунктом 4.4 настоящего Положения;

оценка эффективности системы управления операционным риском;

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

1.3. Коллегиальный исполнительный орган кредитной организации определяет лимиты операционного риска на основе установленных в политике управления операционным риском значений уровней контрольных

показателей путем их распределения по направлениям деятельности (в том числе в разрезе составляющих их банковских процессов), структурным подразделениям, источникам, видам операционного риска, типам событий и видам потерь, на основе подпункта 1.1.1 настоящего пункта приложения.

2. Базовый набор показателей системы управления риском ИБ.

2.1. Количественные показатели системы управления риском ИБ:

2.1.1. Для банков с универсальной и базовой лицензией и НКО:

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 подпунктом 1.1 пункта 1 приложения 2 к настоящему Положению, за определенный период (нарастающим итогом за 3, 6, 9 месяцев и год);

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

отношение суммы прямых потерь, понесенных кредитной организацией за определенный период (нарастающим 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 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 с подпунктом 1.1 пункта 1 приложения 2 к настоящему Положению, за определенный период (нарастающим итогом за 3, 6, 9 месяцев и год) к общей сумме переводов денежных средств и платежами в платежных системах за этот же период (контрольное 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 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 в базе событий событиям риска ИБ с ненулевой величиной прямых потерь в течение отчетного периода, о которых кредитная организация сообщила в своих отчетах в ФинЦЕРТ;

доля выявленных в ходе оценки эффективности 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 подпункте 2.1.1 настоящего пункта 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 (нарастающим итогом за 3, 6, 9 месяцев и год) при выполнении кредитной организацией функций оператора других платежных систем или оператора услуг платежной инфраструктуры к общей сумме операций по переводу денежных средств через другие платежные системы или платежную инфраструктуру 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 эффективности 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» (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2012, № 53, ст. 7592; 2013, № 27,

ст. 3477; № 30, ст. 4084; № 52, ст. 6968; 2014, № 19, ст. 2315, 2317; № 43, ст. 5803; 2015, № 1, ст. 8, 14; 2016, № 27, ст. 4221, 4223; 2017, № 15, ст. 2134; № 18, ст. 2665; № 30, ст. 4456; 2018, № 27, ст. 3950, 3952; № 32, ст. 5115; № 49, ст. 7524), Положением Банка России № 382-П, Положением Банка России № 552-П;

для кредитных организаций – независимая оценка соответствия системы мер в области обеспечения защиты информации по направлениям деятельности (в том числе в разрезе составляющих их банковских процессов) кредитной организации требованиям нормативных актов Банка России, положениям национальных стандартов Российской Федерации и иным требованиям о защите данных, разработанным Банком России в рамках законодательства Российской Федерации о техническом регулировании и стандартизации.

2.3. Участники банковской группы, осуществляющие свою деятельность в иностранных юрисдикциях, в случае противоречия национального законодательства требованиям настоящего Положения, приводят в соответствие с требованиями национального законодательства показатели, указанные в настоящем приложении.

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 подпункта 4.9.1 пункта 4.9 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 ВПОДК в соответствии с Указанием Банка России № 3624-У:

регуляторный подход на базе расчета регуляторного капитала на покрытие операционного риска в соответствии с пунктом 2 Положения Банка России № 652-П и прогнозных сценариев среднегодовых потерь от реализации событий операционного риска, 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 (с использованием статистики за период не менее пяти лет) с использованием методов, применяемых в международной практике.

2. В случае если 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, коллегиальный исполнительный орган кредитной организации в составе материалов на совет директоров (наблюдательный совет) по утверждению стратегии управления рисками и капиталом представляет мотивированное суждение, содержащее обоснование того, что уровень операционного риска в кредитной организации оценивается им ниже, чем требуется в соответствии с регуляторным подходом.

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 компонентов:

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

где:

$К_{\text{необ\_Ki,ОР}}$ – необходимый капитал для целей ВПОДК на покрытие потерь от реализации событий операционного риска, включаемый в состав капитала Ki, определенный в соответствии с методикой, предусмотренной Положением Банка России от 4 июля 2018 года № 646-П «О методике определения собственных средств (капитала) кредитных организаций («Базель III»)», зарегистрированным Министерством юстиции Российской Федерации 10 сентября 2018 года № 52122, 19 декабря 2018 года № 53064;

$К_{\text{мин\_Ki,ОР}}$ – минимальный регуляторный капитал, включаемый в состав капитала Ki и выделяемый на покрытие потерь от реализации событий операционного риска, необходимый для соблюдения минимально допустимого числового значения норматива достаточности капитала Н1.i, определенного в подпункте 2.1.1 пункта 2.1 Инструкции Банка России от 28 июня 2017 года № 180-И «Об обязательных нормативах банков», зарегистрированным Министерством юстиции Российский Федерации 12 июля 2017 года № 47383, 30 ноября 2017 года № 49055, 10 января 2018 года № 49586, 5 апреля 2018 года № 50655, 11 июля 2018 года №51589,

22 августа 2018 года № 51974, 25 сентября 2018 года № 52250, 28 декабря 2018 года № 53224 (далее – Инструкция Банка России № 180-И) с учетом Положения Банка России от 3 декабря 2015 года № 509-П «О расчете величины собственных средств (капитала), обязательных нормативов и размеров (лимитов) открытых валютных позиций банковских групп», зарегистрированного Министерством юстиции Российский Федерации 28 декабря 2015 года № 40318:

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

где:

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

ОР – целевое (прогнозное) значение на планируемый период размера операционного риска, определяемого в соответствии с пунктом 2 Положения Банка России № 652-П;

$Δ_{Ki,ИБ}$ – компонент 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 значением контрольного показателя – лимита прямых (совокупных) годовых потерь от реализации событий риска ИБ), установленного в соответствии с подпунктом 2.1.1 пункта 2 приложения 4 к настоящему Положению;

$Δ_{Ki,ОР}$ – компонент 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 значением контрольного показателя – лимита прямых (совокупных) годовых потерь от реализации событий операционного риска за вычетом лимита прямых потерь от реализации событий риска ИБ, установленного в соответствии с подпунктом 1.1.1 пункта 1.1 приложения 4 к настоящему Положению.

4. В случае 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 рассчитанный для данного года на протяжении последних десяти лет, то кредитная организация приравнивает к нулю компонент необходимого капитала на покрытие потерь от реализации событий риска ИБ и (или) событий операционного риска на базе мотивированного суждения службы управления рисками об отсутствии других факторов возможных потерь, например, отсутствии изменений внутренних и внешних факторов операционной среды кредитной организации с приложением результатов сценарного анализа и стресс-тестирования.

4.1. В случае если у кредитной организации нет данных о потерях от реализации событий операционного риска и событий риска ИБ за десять лет, то кредитная организация использует в целях расчета необходимого капитала накопленные данные за имеющейся период, но не менее трех лет, с учетом включения накопленных данных о потерях последующих лет до достижения периода в десять лет, для сравнения с минимальным регуляторным капиталом за каждый год в течение периода в десять лет.

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 компонентов необходимого капитала на покрытие потерь от реализации событий операционного риска и (или) событий риска ИБ.

4.2. Коллегиальный исполнительный орган кредитной организации рассматривает мотивированное суждение об отсутствии других факторов возможных потерь от операционных рисков и утверждает его в рамках внутренних процедур планирования капитала на покрытие операционного риска.

4.3. В случае 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 устанавливает нулевые значения компонентов $\Delta_{Ki,ИБ}$ и $\Delta_{Ki,ОР}$ и при определении объема необходимого капитала на покрытие операционного риска для целей ВПОДК кредитная организация должна определять значение данных компонентов с учетом сценарного анализа.

4.4. Подразделение, ответственное за организацию управления операционным риском, подготавливает мотивированное суждения об отсутствии других факторов возможных потерь от операционного риска и направляет его на рассмотрение в службу управления рисками.

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 Ki 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 в документах доверительной вероятностью как сумму двух компонентов:

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 анализа, в соответствии с пунктом 4.3 приложения 1 к Указанию Банка России № 3624-У.

6. В случае 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 потерь для целей ВПОДК, то данное превышение добавляется в течение последующего года к оценке компонентов 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 данного года, в котором были отражены потери, при определении сигнального значения прямых или совокупных потерь, уменьшает 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 механизмы и процедуры управления отдельными видами операционного риска, в составе необходимого капитала на покрытие операционного риска для целей ВПОДК выделяет дополнительные компоненты необходимого капитала на покрытие этих видов операционного риска.

Пояснительная записка

к проекту положения Банка России

«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Банк России подготовил новую редакцию проекта положения Банка России «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» (далее – проект Положения) и направляет его на повторное публичное обсуждение с банковским сообществом.

В рамках работы с поступившими предложениями в рамках первичного публичного обсуждения, состоявшегося с 18.09.2018 по 01.10.2018, Банком России проведены совещания с банковским сообществом. По их результатам проект Положения был доработан в части, например, дифференциации требований и сроков внедрения системы управления операционным риском в зависимости от размера активов кредитной организации и типа лицензии, введения единого материального порога на включение события операционного риска в базу событий операционного риска кредитной организации и др.

Целью проекта Положения является установление требований к управлению операционным риском, риском информационной безопасности (включая киберриск), риском информационных систем, требований к политике кредитной организации в сфере информационных технологий, а также установление Банком России подходов к дополнительным требованиям к капиталу, необходимого на покрытие потерь от реализации операционного риска, в том числе риска информационной безопасности (включая киберриск), единых нормативных требований к ведению базы данных о событиях операционного риска и внутренней отчетности кредитных организаций по операционному риску.

Проект Положения является первым нормативным актом, выпускаемым в целях внедрения нового стандартизированного подхода к оценке операционного риска для целей расчета норматива достаточности капитала Базель III[1]. Банк России планирует издание отдельного нормативного акта по внедрению стандартизированного подхода к оценке операционного риска для целей расчета норматива достаточности капитала Базель III в 2020 году.

Проект Положения планируется ввести в действие в течение 10 дней со дня

[1] Basel III: Finalising post-crisis reforms, December 2017.

опубликования с учетом особенностей переходного положения для разных категорий кредитных организаций.

Действие проекта Положения распространяется на кредитные организации и банковские группы, за исключением центрального контрагента, в значении, установленном в статье 2 Федерального закона от 07.02.2011 № 7-ФЗ «О клиринге, клиринговой деятельности и центральном контрагенте».

Банком России проведено соотнесение норм проекта Положения с Указанием Банка России от 15 апреля 2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы», в результате чего проект Положения направляется на повторное публичное обсуждение совместно с проектом Указания Банка России «О внесении изменений в Указание Банка России от 15 апреля 2015 года № 3624-У «О требованиях к системе управления рисками и капиталом кредитной организации и банковской группы».

Ответственным структурным подразделением Банка России за подготовку данного проекта Положения является Департамент банковского регулирования.

Предложения и замечания по проекту Положения принимаются до 4 апреля 2019 года по адресу электронной почты: grigorevps@cbr.ru.