ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

П О Л О Ж Е Н И Е

«8» апреля 2020 г. № 716-П

МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
г. Москва
Регистрационный № 58577
от "03" июня 2020 г.

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; 2013, № 27, ст. 3438; 2019, № 49, ст. 6953) (далее – Федеральный закон № 86-ФЗ) и статьи 11^{1-2} Федерального закона «О банках и банковской деятельности» (в редакции Федерального закона от 3 февраля 1996 года № 17-ФЗ) (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2013, № 27, ст. 3438; 2019, № 49, ст. 6953) (далее – Федеральный закон «О банках и банковской деятельности») Банк России устанавливает требования к системе управления операционным риском в кредитной организации и банковской группе.

Глава 1. **Общие положения**

1.1. Кредитная организация и головная кредитная организация банковской группы, 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; 2016, № 1, ст. 23; 2017, № 30, ст. 4456), и центрального депозитария в значении,

установленном в статье 2 Федерального закона от 7 декабря 2011 года № 414-ФЗ «О центральном депозитарии» (Собрание законодательства Российской Федерации, 2011, № 50, ст. 7356), должны организовать управление операционным риском в соответствии с настоящим Положением.

Понятие «операционный риск» применяется в настоящем Положении в значении, установленном в пункте 4.1 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, 3 июня 2020 года № 58576 (далее – Указание 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 2 настоящего Положения, классифицирует события операционного риска в соответствии с главой 3 настоящего Положения и фиксирует события операционного риска в базе событий в соответствии с главой 6 настоящего Положения. Понятие «база событий» применяется в настоящем Положении в значении, установленном в пункте 4.3 приложения 1 к Указанию Банка России № 3624-У.

1.3. Система управления операционным риском в кредитной организации (головной кредитной организации банковской группы) включает следующие элементы:

процедуры управления операционным риском в соответствии с главой 2 настоящего Положения;

классификатор событий операционного риска, используемый в системе управления операционным риском, в соответствии с главой 3 настоящего Положения;

базу событий;

контрольные показатели уровня операционного риска в соответствии с главой 5 настоящего Положения;

подразделение кредитной организации (головной кредитной организации банковской группы), ответственное за организацию управления операционным риском, структурно входящее в службу управления рисками кредитной организации (головной кредитной организации банковской группы) (далее – подразделение, ответственное за организацию управления операционным риском);

специализированные подразделения кредитной организации (головной кредитной организации банковской группы, участников банковской группы (в последних при наличии), которые в рамках функциональных обязанностей выполняют процедуры управления операционным риском, указанные в подпунктах 2.1.2, 2.1.6 и 2.1.7 пункта 2.1 настоящего Положения, в части отдельных видов операционного риска, определенных в пункте 1.4 настоящего Положения (далее – специализированное подразделение). В случае если специализированные подразделения организационно независимы от службы управления рисками кредитной организации (головной кредитной организации банковской группы), кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок координации руководителем подразделения, ответственного за организацию управления операционным риском, деятельности работников таких специализированных подразделений, связанной с управлением операционным риском, в части соблюдения процедур управления операционным риском, обмена информации, предоставления отчетности и других элементов взаимодействия;

подразделения кредитной организации (головной кредитной организации банковской группы), осуществляющие в рамках системы управления операционным риском идентификацию операционного риска, сбор информации и информирование о выявленном операционном риске как подразделения, ответственного за организацию управления операционным

риском, так и подразделения, в котором выявлен операционный риск (в соответствии с внутренними документами кредитной организации (головной кредитной организации банковской группы) в случае, если операционный риск выявлен в деятельности другого подразделения кредитной организации (головной кредитной организации банковской группы), оценку выявленных операционных рисков (в пределах своей компетенции), разработку и проведение мероприятий, направленных на уменьшение негативного влияния операционного риска, а также мониторинг уровня операционного риска в своих процессах (далее – центры компетенций). К центрам компетенций в рамках системы управления операционным риском относятся подразделения кредитной организации (головной кредитной организации банковской группы), в функциональные обязанности которых входит осуществление операций и сделок в рамках своих процессов и которые несут ответственность за результаты выполнения процесса и за достижение целевых показателей процесса (далее – подразделения, ответственные за осуществление операций и сделок и за результаты процесса), и подразделения, обеспечивающие процессы кредитной организации (головной кредитной организации банковской группы);

подразделение кредитной организации (головной кредитной организации банковской группы), структурно независимое от службы управления рисками (например, служба внутреннего аудита), уполномоченное проводить ежегодную оценку эффективности функционирования системы управления операционным риском, в том числе оценку эффективности выполнения принятых в кредитной организации (головной кредитной организации банковской группы) процедур управления операционным риском, в соответствии с пунктом 4.4 настоящего Положения (далее – уполномоченное подразделение);

автоматизированную информационную систему, объем и функциональность которой определяется осуществляемыми операциями и (или) действующими процессами кредитной организации (головной

кредитной организации банковской группы), обеспечивающую функционирование как в целом системы управления операционным риском, так и отдельных ее элементов (например, базы событий), в том числе сохранность данных и их защиту от искажений;

дополнительные элементы системы управления операционным риском, определенные 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 управления по которым выполняются специализированными подразделениями при участии подразделения, ответственного за организацию управления операционным риском:

риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности кредитной организации (далее – риск информационной безопасности);

риск отказов и (или) нарушения функционирования применяемых кредитной организацией информационных систем и (или) несоответствия их функциональных возможностей и характеристик потребностям кредитной организации (далее – риск информационных систем);

правовой риск в значении, установленном в пункте 3.3 Указания Банка России № 3624-У;

риск ошибок в управлении проектами, состоящий в недостатках и нарушениях организации процессов управления проектной деятельностью, направленных на изменение систем функционирования и поддержания работоспособности кредитной организации;

риск ошибок в управленческих процессах, состоящий в недостатках и нарушениях внутренних процессов кредитной организации, недостатках

принятия решений по банковским сделкам и операциям, внутрихозяйственной деятельности;

риск ошибок в процессах осуществления внутреннего контроля, состоящий в недостатках и нарушениях системы внутреннего контроля, в том числе нарушениях правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, нарушениях внутренних правил совершения операций и сделок;

модельный риск в значении, установленном в пункте 4.2 приложения 1 к Указанию Банка России № 3624-У;

риск потерь средств клиентов, контрагентов, работников и третьих лиц (не компенсированных кредитной организацией) вследствие нарушения кредитной организацией кодексов профессиональной этики, рыночных практик, правил поведения кредитной организации при продаже финансовых инструментов и услуг;

риск ошибок процесса управления персоналом, состоящий в недостатках и нарушениях внутренних процессов кредитной организации в управлении персоналом, в том числе при подборе, найме, адаптации, увольнении, обеспечении безопасности и охраны труда, социальной поддержки, в системе вознаграждения и компенсации;

операционный риск платежной системы в значении, установленном в абзаце третьем пункта 1 приложения 2 к Положению Банка России от 3 октября 2017 года № 607-П «О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков», зарегистрированному Министерством юстиции Российской Федерации 22 декабря 2017 года № 49386 (далее – Положение Банка России № 607-П).

В случае если в кредитной организации (головной кредитной организации банковской группы, участнике банковской группы) отсутствуют

специализированные подразделения, процедуры управления отдельными видами операционного риска выполняет служба управления рисками.

1.5. Кредитная организация (головная кредитная организация банковской группы) утверждает процедуры управления операционным риском в соответствии с пунктом 2.4 Указания Банка России № 3624-У. Единоличный и коллегиальный исполнительные органы кредитной организации (головной кредитной организации банковской группы) обеспечивают их исполнение в соответствии с требованиями главы 2 настоящего Положения. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) несет ответственность за соблюдение требований настоящего Положения.

Глава 2. **Процедуры управления операционным риском**

2.1. Кредитная организация (головная кредитная организация банковской группы) с учетом положений пункта 4.1 приложения 1 к Указанию Банка России № 3624-У и главы 9 настоящего Положения устанавливает во внутренних документах следующие процедуры управления операционным риском.

2.1.1. Идентификация операционного риска, включающая следующие способы:

анализ базы событий;

проведение подразделениями кредитной организации (головной кредитной организации банковской группы) ежегодной самооценки уровня операционного риска и форм (способов) контроля, направленных на снижение его уровня, на основе формализованных анкет (далее – самооценка операционного риска) в соответствии с требованиями абзацев восьмого – тринадцатого подпункта 2.1.5 настоящего пункта;

анализ динамики количественных показателей, направленных на измерение и контроль уровня операционного риска в определенный момент времени (ключевых индикаторов риска) (далее – КИР), по направлениям

деятельности, в том числе в разрезе составляющих их процессов, кредитной организации (головной кредитной организации банковской группы) в соответствии с абзацами девятым – двадцатым подпункта 2.1.7 настоящего пункта;

интервью с работниками кредитной организации (головной кредитной организации банковской группы), в том числе с руководством кредитной организации (головной кредитной организации банковской группы), в рамках которых работниками и руководством кредитной организации (головной кредитной организации банковской группы) обсуждаются операционные риски, оказывающие влияние на деятельность кредитной организации (головной кредитной организации банковской группы);

анализ актов проверок, судебных актов (решений, определений, постановлений) и (или) актов исполнительных органов государственной власти, Банка России в части фактов, относящихся к реализации операционного риска;

анализ информации уполномоченного подразделения и внешнего аудита;

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

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

Кредитная организация (головная кредитная организация банковской группы) использует результаты процедуры идентификации операционного риска для проведения процедур количественной и качественной оценки уровня операционного риска и корректного учета связи идентифицированного операционного риска с событиями операционного риска в базе событий.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок ведения реестра операционных рисков с использованием элементов классификации, указанных в пункте 3.1 настоящего Положения.

2.1.2. Сбор и регистрация информации о внутренних событиях операционного риска и потерях от его реализации, включающие следующие способы:

автоматизированное выявление информации из информационных систем о реализовавшихся или возможных в будущем событиях операционного риска;

неавтоматизированное выявление и сбор информации о событиях операционного риска, предусматривающие с использованием экспертного мнения выявление информации и проведение анализа обстоятельств и причин произошедших событий операционного риска, в случае, если автоматизированное выявление и сбор информации о событиях операционного риска невозможны. Порядок и срок проведения анализа обстоятельств и причин произошедших событий операционного риска определяется кредитной организацией (головной кредитной организации банковской группы) во внутренних документах;

ввод информации о событиях операционного риска в базу событий по алгоритмизированным правилам, установленным кредитной организацией (головной кредитной организации банковской группы) во внутренних документах;

классификацию выявленных событий операционного риска в соответствии с главой 3 настоящего Положения;

определение потерь от реализации событий операционного риска в соответствии с подпунктом 2.1.3 настоящего пункта;

регистрацию событий операционного риска в базе событий;

определение стоимости возмещений потерь от реализации событий операционного риска в базе событий;

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

актуализацию источников информации о событиях операционного риска и сведений о центрах компетенций, ответственных за их сбор.

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 том числе в разрезе составляющих их процессов, с указанием во внутренних документах:

центров компетенций;

правил предоставления информации об идентифицированных событиях операционного риска центрами компетенций в подразделение, ответственное за организацию управления операционным риском, не позднее пяти рабочих дней с момента идентификации события операционного риска, за исключением событий операционного риска, загружаемых в базу событий программно-аппаратными средствами на определенную кредитной организацией (головной кредитной организацией банковской группы) отчетную дату в соответствии с порядком, указанным кредитной организаций (головной кредитной организацией банковской группы) во внутренних документах, но не реже одного раза в месяц (предоставление информации об идентифицированных событиях операционного риска дочерней кредитной организацией в головную кредитную организацию банковской группы осуществляется в соответствии с пунктом 6.3 настоящего Положения);

контрольных показателей уровня операционного риска, указанных в абзацах втором и седьмом подпункта 1.1.1 и абзацах втором и девятом подпункта 1.2.1 пункта 1 приложения 1 к настоящему Положению в разрезе центров компетенций (ключевых показателей эффективности по выявлению событий операционного риска в процессах), ответственность за несоблюдение которых возложена на центры компетенций (их руководителей).

2.1.3. Определение потерь и возмещений потерь от реализации событий операционного риска, включающее следующие способы:

учет потерь кредитной организации (головной кредитной организации банковской группы), указанных в пункте 3.11 настоящего Положения, включая установление сроков выявления и правил отражения в бухгалтерском учете, с учетом пунктов 6.7–6.19 настоящего Положения;

порядок и методы определения потерь кредитной организации (головной кредитной организации банковской группы), указанных в пункте 3.13 настоящего Положения, от события операционного риска;

порядок выявления расходов, относящихся к операционному риску, из общих расходов кредитной организации (головной кредитной организации банковской группы) (для определения потерь, указанных в пункте 3.12 настоящего Положения), в том числе порядок выявления и сверки событий операционного риска с данными бухгалтерского учета;

порядок и методы оценки недополученных доходов, связанных с событиями операционного риска (для определения потерь, указанных в пункте 3.13 настоящего Положения);

порядок и методы определения потенциальных потерь, указанных в подпункте 3.13.3 пункта 3.13 настоящего Положения;

порядок и методы определения стоимости возмещений от событий операционного риска;

отбор и назначение экспертов кредитной организации (головной кредитной организации банковской группы), ответственных за расчет потерь от реализации событий операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, областей их компетенции и ответственности. Допускается совмещение функции регистрации событий операционного риска в базе событий и функции расчета потерь и возмещений от реализации событий операционного риска.

2.1.4. Количественная оценка уровня операционного риска, включающая следующие способы:

агрегированную оценку уровня операционного риска по кредитной организации (головной кредитной организации банковской группы) в целом, по подразделениям кредитной организации (головной кредитной организации банковской группы), а также по типам событий операционного риска в соответствии с пунктом 3.6 настоящего Положения, направлениям деятельности, в том числе в разрезе составляющих их процессов, в соответствии с пунктом 3.9 настоящего Положения и видам операционного риска в соответствии с пунктом 1.4 настоящего Положения;

оценку объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) в рамках внутренних процедур оценки достаточности капитала (далее – ВПОДК), на покрытие потерь от реализации событий операционного риска в целом по кредитной организации (головной кредитной организации банковской группы) в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, риска информационной безопасности и других видов операционного риска, с учетом подходов к расчету объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации операционного риска, изложенных в приложении 2 к настоящему Положению;

оценку ожидаемых потерь от реализации операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, по которым наблюдается статистика событий операционного риска, в целях покрытия этих потерь за счет ценообразования услуг и тарифов (при наличии). Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах методы и порядок проведения оценки ожидаемых потерь от реализации операционного риска.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает во внутренних документах способы проведения процедуры количественной оценки уровня операционного риска, в том числе с использованием средств автоматизации.

2.1.5. Качественная оценка уровня операционного риска, проводимая в отношении выявленных операционных рисков в дополнение к количественной оценке и включающая следующие способы:

самооценку операционного риска в соответствии с абзацами восьмым – тринадцатым настоящего подпункта;

профессиональную оценку выделенными для данной процедуры работниками подразделений кредитной организации (головной кредитной организации банковской группы) и (или) внешними экспертами с учетом установленных кредитной организацией (головной кредитной организации банковской группы) во внутренних документах правил привлечения внешних экспертов;

сценарный анализ операционных рисков.

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

Подразделение, ответственное за организацию управления операционным риском, разрабатывает на ежегодной основе план мероприятий по проведению качественной оценки уровня операционного риска, который утверждается коллегиальным исполнительным органом кредитной организации (головной кредитной организации банковской группы) и включает определение ответственных и участвующих подразделений кредитной организации (головной кредитной организации банковской группы) (далее – план проведения качественной оценки).

Подразделения кредитной организации (головной кредитной организации банковской группы) осуществляют оценку уровня операционного риска в соответствии с планом проведения качественной оценки.

Самооценка операционного риска проводится кредитной организацией (головной кредитной организацией банковской группы) не реже одного раза в

год по установленной во внутренних документах методике (в виде анкетирования выделенных для данной процедуры работников подразделений кредитной организации (головной кредитной организации банковской группы) по всем направлениям деятельности, в том числе в разрезе составляющих их процессов, с использованием формализованных анкет).

Самооценка операционного риска проводится кредитной организацией (головной кредитной организацией банковской группы) в отношении всех видов операционного риска в соответствии с планом проведения качественной оценки.

Кредитная организация (головная кредитной организации банковской группы) определяет критерии самооценки операционного риска, которые должны включать:

критерии оценки уровня существенности операционного риска (с соотнесением к четырехуровневой шкале: «очень высокий», «высокий», «средний», «низкий»), включая критерии оценки потерь и вероятности операционного риска в условиях текущего процесса;

критерии оценки эффективности форм (способов) контроля (с учетом уровня регламентации и автоматизации мер уменьшения негативного влияния оцениваемого операционного риска), действующих на момент проведения оценки;

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

Кредитная организация (головная кредитная организация банковской группы) разрабатывает требования к проведению профессиональной оценки уровня операционного риска выделенными для данной процедуры работниками подразделений кредитной организации (головной кредитной организации банковской группы) и (или) внешними экспертами с указанием сроков, правил и порядка ее проведения.

Кредитная организация (головная кредитная организация банковской группы) разрабатывает во внутренних документах методы проведения профессиональной оценки уровня операционного риска выделенными для данной процедуры работниками подразделений кредитной организации (головной кредитной организации банковской группы) на основе требований к ее проведению.

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

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

2.1.6. Выбор и применение способа реагирования на операционный риск по результатам мероприятий, утвержденных в соответствии с абзацем шестым подпункта 2.1.5 настоящего пункта, в срок не более трех месяцев со дня проведения оценки уровня операционного риска, включая следующие способы реагирования:

уклонение от риска, предусматривающее отказ кредитной организации (головной кредитной организации банковской группы) от оказания соответствующего вида услуг и операций в связи с высоким уровнем операционного риска в них;

передачу риска, предусматривающую страхование, передачу риска другой стороне – контрагенту и (или) клиенту;

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

принятие мер, направленных на уменьшение негативного влияния операционного риска на качество процессов, величины совокупных потерь от реализации операционного риска до учета возмещения (далее – валовые потери), включая разработку кредитной организацией (головной кредитной организации банковской группы) форм (способов) контроля, которые включают:

изменения, вносимые в процессы;

установление дополнительных форм (способов) контроля;

обучение работников, в том числе участников процессов;

применение автоматизированных решений;

другие меры, направленные на уменьшение негативного влияния операционного риска.

Рекомендуемый перечень возможных мер, направленных на уменьшение негативного влияния операционного риска, приведен в приложении 3 к настоящему Положению.

Кредитная организация (головная кредитная организация банковской группы) выбирает и применяет способы реагирования на операционный риск в зависимости от оценки уровня операционного риска, в том числе уровня потерь от реализации операционного риска и событий операционного риска.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок проведения процедуры выбора и применения способа реагирования на операционный риск, в том числе методы оценки стоимости выбранного способа реагирования.

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

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

2.1.7. Мониторинг операционного риска, включающий следующие способы:

установление и мониторинг КИР;

анализ статистики событий операционного риска, в том числе причин возникновения событий операционного риска и потерь от их реализации;

контроль выполнения мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, включая мероприятия, направленные на предотвращение (снижение вероятности) событий операционного риска, и мероприятия, направленные на ограничение размера потерь от реализации событий операционного риска, определенных в соответствии с подпунктом 4.1.5 пункта 4.1 настоящего Положения;

контроль выполнения мер, направленных на уменьшение негативного влияния операционного риска, определенных в соответствии с абзацами пятым – десятым подпункта 2.1.6 настоящего пункта;

контроль соблюдения выбранных способов реагирования на операционные риски;

мониторинг потоков информации в рамках реализации операционного риска, поступающей от подразделений кредитной организации (головной кредитной организации банковской группы) и центров компетенций, единоличного и коллегиального органов управления кредитной организации (головной кредитной организации банковской группы), из других источников информации.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах процедуру мониторинга операционного риска.

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

Кредитная организация (головная кредитная организация банковской группы) во внутренних документах устанавливает требования к КИР и к их документированию, включающие:

количественное измерение КИР;

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

периодичность (не реже одного раза в год) 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 ее источников, включая способ получения информации;

пороговые значения КИР с обоснованием их установления;

наименования и элементы классификации операционных рисков, которые отслеживают КИР;

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

порядок реагирования на превышение пороговых значений КИР.

Для кредитных организаций (головных кредитных организаций банковской группы), являющихся в соответствии со статьей 3 Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе»

(Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 31, ст. 4423) (далее – Федеральный закон № 161-ФЗ) операторами платежной системы или операторами услуг платежной инфраструктуры, требования к КИР должны быть установлены с учетом требований к определению показателей бесперебойности функционирования платежной системы, установленных в приложении 1 к Положению Банка России № 607-П, которые должны рассматриваться в качестве КИР.

Кредитная организация (головная кредитная организация банковской группы) направляет результаты процедуры мониторинга операционного риска на рассмотрение коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы) или другим органам кредитной организации (головной кредитной организации банковской группы), перечень которых определяется во внутренних документах кредитной организации (головной кредитной организации банковской группы), в составе ежеквартального и годового отчетов об управлении операционным риском в соответствии с абзацем вторым и третьим подпункта 4.2.2 и подпунктом 4.2.3 пункта 4.2 настоящего Положения.

2.2. Кредитная организация (головная кредитная организация банковской группы) предусматривает во внутренних документах, регламентирующих процедуры управления операционным риском, функции и обязанность подразделений кредитной организации (головной кредитной организации банковской группы), участвующих на различных этапах процессов (далее – подразделение – участник процессов), а также подразделений, ответственных за осуществление операций и сделок и за результаты процесса, участвовать в выявлении операционного риска и сборе информации о событиях операционного риска и потерях от его реализации, в качественной оценке операционного риска.

2.3. Кредитная организация (головная кредитная организация банковской группы) включает информацию о результатах проведения процедур управления операционным риском, установленных пунктом 2.1

настоящего Положения, в состав ежеквартального и годового отчетов об управлении операционным риском в соответствии с абзацем вторым подпункта 4.2.2 и подпунктом 4.2.3 пункта 4.2 настоящего Положения.

2.4. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах, регламентирующих процедуры управления операционным риском, способы их проведения, перечисленные в настоящей главе, с учетом требований, указанных в главе 9 настоящего Положения.

2.5. Оценка эффективности выполнения процедур управления операционным риском кредитной организации (головной кредитной организации банковской группы) производится уполномоченным подразделением с учетом требований подпункта 4.1.4 пункта 4.1, пунктов 4.4, 4.6, 6.12, 6.17, 6.19, 7.11, 8.4, подпункта 8.8.8 пункта 8.8 и главы 9 настоящего Положения и приложения 1 к настоящему Положению. 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 во внутренних документах кредитной организации (головной кредитной организации банковской группы).

Глава 3. **Классификатор событий операционного риска**

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

3.2. Кредитная организация (головная кредитная организация банковской группы) для всех видов операционного риска определяет во внутренних документах единый классификатор событий операционного риска в разрезе элементов, перечисленных в пункте 3.1 настоящего Положения. Единый классификатор событий операционного риска должен обновляться кредитной организацией (головной кредитной организации банковской группы) с учетом изменений осуществляемых операций и (или) действующих процессов кредитной организации (головной кредитной организации банковской группы).

3.3. Источники операционного риска классифицируются кредитной организацией (головной кредитной организацией банковской группы) на следующие категории.

3.3.1. К первой категории относятся недостатки процессов, в том числе ненадежная и (или) неэффективная организация внутренних процессов управления в кредитной организации и совершения банковских и других операций, а также несоответствие указанных процессов деятельности кредитной организации и (или) требованиям законодательства Российской Федерации (далее – недостатки процессов);

3.3.2. Ко второй категории относятся недостатки, 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 агентских отношений по выполнению работ (оказанию услуг) от лица кредитной организации в соответствии со статьей 64^1 Федерального закона № 86-ФЗ (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2780; 2013, № 27, ст. 3438; 2017, № 18, ст. 2669) (далее – действия персонала и других связанных с кредитной организацией лиц);

3.3.3. К третьей категории относятся отказы и (или) нарушения функционирования применяемых кредитной организацией информационных,

технологических и других систем, оборудования и (или) несоответствие их функциональных возможностей и характеристик потребностям кредитной организации (далее – сбои систем и оборудования);

3.3.4. К четвертой категории относится воздействие внешних причин, включая действия третьих лиц, в том числе действия суда и исполнительных органов государственной власти, Банка России, других организаций, а также другие воздействия внешнего характера (далее – внешние причины).

3.4. Кредитная организация (головная кредитная организация банковской группы) во внутренних документах определяет последующие уровни классификации источников событий операционного риска.

3.5. У одного и того же события операционного риска может быть один источник или несколько источников операционного риска. В случае если кредитной организацией (головной кредитной организацией банковской группы) определено более одного источника операционного риска, в отношении реализовавшегося события операционного риска в базе событий кредитная организация (головная кредитная организация банковской группы) указывает все выявленные источники события операционного риска и определяет наиболее значимый источник операционного риска.

3.6. Классификация типов событий операционного риска осуществляется кредитной организацией (головной кредитной организацией банковской группы) следующим образом:

3.6.1. совершение работниками кредитной организации и другими связанными с кредитной организацией лицами, включая собственников, а также физическими лицами, связанными с кредитной организацией в рамках агентских отношений по выполнению работ (оказанию услуг) от лица кредитной организации, преднамеренных действий или преднамеренное бездействие указанных лиц, направленные на присвоение, хищение, уничтожение, нанесение ущерба материальным и нематериальным активам или другому имуществу кредитной организации и (или) средствам клиентов, нарушение процессов, препятствующие достижению целей кредитной

организации, в том числе умышленное несоблюдение нормативных актов или внутренних документов кредитной организации в целях извлечения материальной и нематериальной выгоды (далее – преднамеренные действия персонала);

3.6.2. совершение третьими лицами преднамеренных действий, направленных на присвоение, хищение, уничтожение, нанесение ущерба материальным и нематериальным активам или другому имуществу кредитной организации и (или) средствам клиентов (за исключением вандализма), нарушение процессов и ухудшение работы систем, препятствующих достижению стратегии развития кредитной организации или нарушающих законодательство Российской Федерации, в том числе приобретение прав на имущество кредитной организации обманным путем (далее – преднамеренные действия третьих лиц);

3.6.3. нарушение со стороны кредитной организации трудового законодательства, кадровой политики, условий труда и безопасности, требований по охране труда или охране здоровья, связанных с выплатами работникам кредитной организации по исковым требованиям (в том числе по искам о возмещении морального и материального вреда или искам в связи с дискриминацией), а также вследствие прекращения трудовых отношений (далее – нарушение кадровой политики и безопасности труда);

3.6.4. нарушение со стороны кредитной организации прав клиентов и контрагентов, включая нанесение им ущерба, при оказании им услуг и совершении операций, включая нарушение условий договоров и сохранности конфиденциальной информации, ставшей доступной кредитной организации в процессе взаимодействия с клиентами и контрагентами по операциям и сделкам при оказании услуг, предоставлении банковских услуг с условием приобретения клиентом сопутствующих услуг кредитной организации или третьих лиц и нарушение законодательства в сфере защиты прав потребителей, а также антимонопольного законодательства (далее – нарушение прав клиентов и контрагентов);

3.6.5. ущерб материальным активам кредитной организации вследствие снижения стоимости имущества, потери свойств материальных активов кредитной организации в результате стихийных бедствий, техногенных катастроф, эпидемий, беспорядков, вандализма и военных действий (далее – ущерб материальным активам);

3.6.6. нарушение и сбои систем и оборудования, обеспечивающих функционирование деятельности кредитной организации (далее – нарушение и сбои систем и оборудования);

3.6.7. нарушение организации, исполнения и управления процессами кредитной организации, включая ошибки при обработке операций, недостатки обеспечения функционирования процессов, недостатки систем управления рисками, внутреннего контроля, учета и отчетности, системы обеспечения информационной безопасности, недостатки внутренних 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 3.6.1 настоящего пункта (далее – нарушение организации, исполнения и управления процессами).

3.7. Для отдельных видов операционного риска в целях классификации событий операционного риска в базе событий кредитной организацией (головной кредитной организацией банковской группы) применяются дополнительные типы событий операционного риска в разрезе классификации типов событий в соответствии с пунктом 3.6 настоящего Положения.

3.8. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах детализированную классификацию типов событий операционного риска в соответствии с приложением 4 к настоящему Положению, а также вправе определить более детализированную классификацию типов событий операционного риска с

учетом осуществляемых операций и (или) действующих процессов кредитной организации (головной кредитной организации банковской группы).

3.9. События операционного риска классифицируются кредитной организацией (головной кредитной организации банковской группы) по основным направлениям деятельности первого уровня следующим образом:

3.9.1. оказание услуг юридическим лицам, органам государственной власти и местного самоуправления по организации доступа к рынкам капитала, оптимизации структуры активов и повышению качества корпоративного управления, слияниям и поглощениям, оказанию консультационных услуг финансового посредничества, в том числе при организации синдицированного кредитования (корпоративное финансирование);

3.9.2. осуществление операций и сделок с финансовыми инструментами торгового портфеля (операции и сделки на финансовом рынке);

3.9.3. оказание банковских услуг розничным клиентам, кроме брокерских и депозитарных услуг (розничное банковское обслуживание);

3.9.4. оказание юридическим лицам банковских услуг, за исключением основного направления деятельности первого уровня, указанного в подпункте 3.9.1 настоящего пункта (коммерческое банковское обслуживание корпоративных клиентов);

3.9.5. осуществление переводов денежных средств, платежей и расчетов через платежные системы, в том числе платежную систему Банка России, в которых кредитная организация выступает как оператор по переводу денежных средств, в том числе платежей по собственным операциям, за исключением внутрибанковских операций по организации услуг по проведению платежей, расчетов и взаимодействия с клиентом в рамках предоставления банковских услуг, относящихся к основным направлениям деятельности первого уровня, указанным в подпунктах 3.9.3, 3.9.4, 3.9.6–3.9.8 настоящего пункта (осуществление переводов денежных средств, платежей и расчетов через платежные системы);

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

3.9.7. управление активами клиентов по договорам доверительного управления (управление активами);

3.9.8. брокерское обслуживание розничных клиентов (розничное брокерское обслуживание);

3.9.9. 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 (обеспечение деятельности кредитной организации).

3.10. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах классификацию направлений деятельности, в том числе в разрезе составляющих их процессов, до второго уровня и далее с учетом осуществляемых операций и (или) действующих процессов кредитной организации (головной кредитной организации банковской группы).

3.11. Виды потерь от реализации событий операционного риска подразделяются кредитной организацией (головной кредитной организацией банковской группы) на прямые и непрямые потери.

3.12. Прямые потери, отраженные на счетах по учету расходов, 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 кредитной организацией (головной кредитной организацией банковской группы) по следующим видам.

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

потеря активов, за исключением наличных денежных средств, в результате хищения;

потеря наличных денежных средств в результате хищения или физического уничтожения;

обесценение стоимости кредита в результате начисления дополнительных резервов в соответствии с Положением Банка России от 28 июня 2017 года № 590-П «О порядке формирования кредитными организациями резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности», зарегистрированным Министерством юстиции Российской Федерации 12 июля 2017 года № 47384, 3 октября 2018 года № 52308, 19 декабря 2018 года № 53053, 23 января 2019 года № 53505, 12 сентября 2019 года № 55910, 27 ноября 2019 года № 56646 (далее – Положение Банка России № 590-П), Положением Банка России от 23 октября 2017 года № 611-П «О порядке формирования кредитными организациями резервов на возможные потери», зарегистрированным Министерством юстиции Российской Федерации 15 марта 2018 года № 50381, 19 декабря 2018 года № 53054, 12 сентября 2019 года № 55911 (далее – Положение Банка России № 611-П), и Указанием Банка России от 22 июня 2005 года № 1584-У «О формировании и размере резерва на возможные потери под операции кредитных организаций с резидентами офшорных зон», зарегистрированным Министерством юстиции Российской Федерации 15 июня 2005 года № 6799 (далее – Указание Банка России № 1584-У), в случае увеличения кредитного риска из-за реализации события операционного риска;

расходы на создание резервов по счетам бухгалтерского учета для покрытия потерь от реализации события операционного риска с учетом видов резервов, за исключением резервов, приведенных в абзаце пятом подпункта 3.12.6 настоящего пункта;

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

потери, отраженные на счетах бухгалтерского учета, отнесенных к счетам расходов;

расходы, связанные с мероприятиями по возврату кредитных средств и других финансовых активов, возникшими по причине операционного риска;

отрицательная переоценка стоимости торгового портфеля и (или) финансового инструмента в части, обусловленной нарушением правил совершения сделок и операций с инструментами торгового портфеля, правил совершения операций, определенных во внутренних документах кредитной организации (например, нарушение лимита сделки);

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

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

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

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

3.12.5. 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.

3.12.6. Расходы (выплаты), связанные с решениями суда и (или) представительством кредитной организации в судах по делам, связанным с потерями от реализации событий операционного риска, включающие:

расходы на работников кредитной организации, представляющих интересы кредитной организации в суде по делам, связанным с реализацией событий операционного риска, не включая расходы на фонд оплаты труда;

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

расходы на адвокатов и судебных представителей по делам (в случае отказа суда от удовлетворения иска в целом или в части) в величине потерь от реализации событий операционного риска;

начисление резервов по прочим потерям и резервов – оценочных обязательств некредитного характера в соответствии с пунктом 6.1 Положения Банка России № 611-П по предъявленным претензиям и судебным искам.

3.12.7. Штрафы, наложенные исполнительными органами государственной власти и (или) Банком России.

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

3.12.9. Отрицательный финансовый результат от невыгодных для кредитной организации сделок, совершенных по причине операционного риска.

3.12.10. Прочие потери, связанные с реализацией события операционного риска или устранением последствий события операционного риска.

3.13. Непрямые потери кредитной организации (головной кредитной организации банковской группы с учетом влияния событий операционного риска участников банковской группы), не отраженные в бухгалтерском учете, но косвенно связанные с событиями операционного риска, классифицируются

кредитной организацией (головной кредитной организации банковской группы) на потери, определяемые расчетным методом в денежном выражении (далее – косвенные потери), потери, определяемые с использованием экспертного мнения (далее – качественные потери) в случае, если потери не выражены в денежном выражении расчетным способом, а также потери кредитной организации, не реализовавшиеся в виде прямых и косвенных потерь, которые могли бы возникнуть при реализации не выявленных кредитной организацией источников операционного риска и (или) при неблагоприятном стечении обстоятельств (например, нарушение работником кредитной организации лимита, которое при данном стечении обстоятельств не привело к прямым потерям в результате реализации события операционного риска) (далее – потенциальные потери).

3.13.1. Косвенные потери включают в себя:

недополученные доходы от приостановления или прекращения совершения операций, вызванных событиями операционного риска (например, приостановления или прекращения работы систем, оборудования);

неполученные доходы, связанные с непроведением отдельных сделок и операций по причине реализации событий операционного риска, не связанных с приостановлением и (или) прекращением совершения операций;

повышение стоимости заимствований, например, стоимости привлечения кредитных средств, в результате события операционного риска;

снижение рыночной стоимости акций кредитной организации или инструментов капитала кредитной организации по причине реализации события операционного риска;

потери, связанные с восстановлением ликвидности из-за оттока денежных средств по причине реализации операционного риска;

прочие потери, связанные с устранением последствий или снижением потерь от реализации операционного риска, за исключением потерь, определенных в соответствии с подпунктами 3.12.8 и 3.12.10 пункта 3.12 настоящего Положения.

3.13.2. Качественные потери включают в себя:

возникновение источников других видов риска (например, кредитного риска, рыночного риска, риска ликвидности, риска потери деловой репутации, регуляторного риска, стратегического риска);

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

отток клиентов;

неисполнение обязательств по сделке и (или) неоказание услуги;

ограничения, приводящие к выполнению невыгодных для кредитной организации действий, накладываемые со стороны суда, исполнительных органов государственной власти, Банка России;

снижение качества предоставления услуг, выполнения операций (например, нарушение регламентированных сроков выполнения процессов и операций, установленных во внутренних документах кредитной организации);

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

судебные акты (решения, определения, постановления), акты исполнительных органов государственной власти, Банка России, не связанные с уплатой штрафов;

снижение лимитов на межбанковское кредитование;

другие качественные потери.

Кредитная организация (головная кредитная организация банковской группы) проводит оценку значимости качественных потерь в соответствии с установленной во внутренних документах кредитной организации (головной кредитной организации банковской группы) шкалой качественных оценок (например, по четырехуровневой шкале: «очень высокие», «высокие», «средние», «низкие»).

Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах критерии шкалы качественных оценок и методику определения оценок для качественных

потерь от реализации события операционного риска, включая критерии соотнесения шкалы качественных оценок с количественными потерями.

3.13.3. Потенциальные потери включают в себя:

потери (в том числе хищение) средств клиентов, контрагентов, работников и третьих лиц, которые не были компенсированы кредитной организацией, с учетом положений абзаца восьмого пункта 6.5 настоящего Положения, включая потери средств физических лиц, в том числе индивидуальных предпринимателей, юридических лиц, штрафы, наложенные на должностных лиц кредитной организации;

другие потенциальные потери.

3.14. В случае если кредитная организация (головная кредитная организация банковской группы) использует дополнительную классификацию видов потерь, кредитная организация (головная кредитная организация банковской группы) устанавливает их во внутренних документах, включая порядок их определения и актуализации.

3.15. Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах методы и порядок определения прямых и непрямых потерь, порядок отнесения расходов кредитной организации (головной кредитной организацией банковской группы) по событиям операционного риска.

Глава 4. Дополнительные элементы системы управления операционным риском

4.1. Система управления операционным риском в кредитной организации (головной кредитной организации банковской группы) в дополнение к элементам, предусмотренным в пункте 1.3 настоящего Положения, включает следующие элементы.

4.1.1. Перечень процессов кредитной организации (головной кредитной организации банковской группы), отнесенных к направлениям деятельности (в разрезе составляющих их процессов), приведенным в пункте 3.9 настоящего

Положения, с указанием уровня их критичности, функций подразделений, ответственных за осуществление операций и сделок и за результаты процесса, и подразделений – участников процессов.

По уровню критичности процессы кредитной организации (головной кредитной организации банковской группы) подразделяются на критически важные процессы, основные, обеспечивающие и прочие.

Критически важные процессы обеспечивают выполнение операций кредитной организации (головной кредитной организации банковской группы), указанных в пунктах 1–4 и 9 части первой статьи 5 Федерального закона «О банках и банковской деятельности» (Ведомости Съезда народных депутатов РСФСР и Верховного Совета РСФСР, 1990, № 27, ст. 357; Собрание законодательства Российской Федерации, 1996, № 6, ст. 492; 2019, № 30, ст. 4151), ведение бухгалтерского учета, представление отчетности в Банк России в соответствии с Указанием 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», зарегистрированным Министерством юстиции Российской Федерации 13 декабря 2018 года № 52992, 13 декабря 2019 года № 56796 (далее – Указание Банка России № 4927-У), поддержание ликвидности, выполнение операций на финансовых рынках, кассовых операций, работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций, соблюдение требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2018, № 1, ст. 82), Трудового кодекса Российской Федерации (Собрание законодательства Российской Федерации, 2002, № 1, ст. 3; 2019, № 51, ст. 7491), Федерального закона «О банках и банковской деятельности», а также другие процессы, которые определены кредитной организацией (головной кредитной организацией банковской группы) и прерывание функционирования которых оказывает влияние на выполнение обязательств перед клиентами и

контрагентами кредитной организации (головной кредитной организации банковской группы).

Основные процессы обеспечивают выполнение операций, предусмотренных статьей 5 Федерального закона «О банках и банковской деятельности», не отнесенных кредитной организацией (головной кредитной организацией банковской группы) к критически важным процессам, и других операций и услуг, объем которых формирует объем расходов (доходов) более 5 процентов от дохода за год для целей расчета капитала на покрытие операционного риска кредитной организации (головной кредитной организации банковской группы), определяемого 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) (далее – доход за год для целей расчета капитала на покрытие операционного риска). Кредитная организация (головная кредитная организация банковской группы) проводит регулярный (не реже одного раза в год) анализ необходимости пересмотра перечня основных процессов при осуществлении действий, предусмотренных пунктом 4.6 настоящего Положения.

К прочим процессам относятся процессы, не отнесенные кредитной организацией (головной кредитной организацией банковской группы) к критически важным процессам или основным процессам.

4.1.2. Политика управления операционным риском и внутренние документы, описывающие процедуры управления операционным риском, а также процедуры оценки эффективности функционирования системы управления операционным риском.

4.1.3. Внутренние документы, устанавливающие в кредитной организации (головной кредитной организации банковской группы) структуру и организацию системы управления операционным риском, в том числе полномочия и функции руководителей подразделения, ответственного за

организацию управления операционным риском, специализированных подразделений, центров компетенций с учетом исключения конфликта интересов.

Дочерние кредитные организации должны согласовывать внутренние документы по структуре и организации системы управления операционным риском, а также внутренние документы, указанные в подпункте 4.1.2 настоящего пункта, с головной кредитной организацией банковской группы.

4.1.4. Порядок оценки уполномоченным подразделением и (или) организацией, осуществляющей внешний аудит, эффективности функционирования системы управления операционным риском, в том числе выполнения принятых в кредитной организации (головной кредитной организации банковской группы) процедур управления операционным риском.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах уполномоченное подразделение, а также правила привлечения для оценки эффективности функционирования системы управления операционным риском внешних экспертов.

4.1.5. Комплекс мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, включая мероприятия, направленные на предотвращение и (или) снижение вероятности событий операционного риска, и мероприятия, направленные на ограничение размера потерь от реализации событий операционного риска.

Мероприятия, направленные на предотвращение и (или) снижение вероятности событий операционного риска, включают:

реализацию кредитной организацией (головной кредитной организацией банковской группы) способов контроля, например, указанных в пунктах 10, 11, 15, 17, 18, 28 приложения 3 к настоящему Положению, на этапах процессов, в которых выявлены операционные риски;

изменение кредитной организацией (головной кредитной организацией банковской группы) процессов и распределение обязанностей для обеспечения исключения конфликта интересов;

документирование кредитной организацией (головной кредитной организацией банковской группы) результатов выполнения процедур контроля в процессах;

обеспечение кредитной организацией (головной кредитной организацией банковской группы) контроля совершения операций и сделок;

исключение совершения неконтролируемых кредитной организацией (головной кредитной организацией банковской группы) операций и сделок;

другие мероприятия, разрабатываемые кредитной организацией (головной кредитной организацией банковской группы) в зависимости от вида и характеристик процесса.

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

установление кредитной организацией (головной кредитной организацией банковской группы) пороговых значений в отношении полномочий принятия решений и определения лимитов операционного риска, контроля за соблюдением полномочий;

внедрение кредитной организацией (головной кредитной организацией банковской группы) элементов автоматизации участков процессов, при выполнении которых выявлены операционные риски по причине ошибок работников;

разработку кредитной организацией (головной кредитной организацией банковской группы) планов по обеспечению непрерывности и (или) восстановления критически важных процессов и функционирования информационных систем, включая автоматизированные системы, программные и (или) программно-аппаратные средства, телекоммуникационное оборудование и линии связи, эксплуатация и использование которых обеспечивается кредитной организацией (головной кредитной организацией

банковской группы) для осуществления процессов и операций (далее – объекты информационной инфраструктуры), а также планов по обеспечению безопасности и целостности информационных систем и информации, в том числе в соответствии с требованиями главы 8 настоящего Положения, с учетом внешних факторов, влияющих на критически важный процесс и (или) информационную систему, в случае реализации операционного риска, включая систему быстрого реагирования на события операционного риска;

определение способа и порядка возмещения потерь от реализации событий операционного риска, например, с использованием переноса риска на участников финансового рынка, страхования;

юридическое обеспечение судебных процессов с участием кредитной организации (головной кредитной организации банковской группы);

юридическое сопровождение процессов, договоров и документации кредитной организации (головной кредитной организации банковской группы);

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

Кредитная организация (головная кредитная организация банковской группы) в зависимости от осуществляемых операций и (или) действующих процессов определяет во внутренних документах комплекс мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска.

Головная кредитная организация банковской группы должна обеспечить выполнение комплекса мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, реализуемого у участников банковской группы.

4.1.6. Способы мотивации работников кредитной организации (головной кредитной организации банковской группы) к совершению следующих действий при участии в управлении операционным риском:

инициативное информирование работниками кредитной организации (головной кредитной организации банковской группы) о возможных операционных рисках и выявленных событиях операционного риска;

участие работников кредитной организации (головной кредитной организации банковской группы) в процедурах управления операционным риском, указанных в главе 2 настоящего Положения;

направление работниками кредитной организации (головной кредитной организации банковской группы) предложений по мероприятиям, направленным на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска;

реализация работниками кредитной организации (головной кредитной организации банковской группы) мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, указанных в подпункте 4.1.5 настоящего пункта;

другие действия работников кредитной организации (головной кредитной организации банковской группы) по участию в управлении операционным риском.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах способы мотивации работников кредитной организации (головной кредитной организации банковской группы) в участии в управлении операционным риском, включающие требование соблюдения 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 подпункте.

4.1.7. Отчеты по операционному риску и информация о событиях операционного риска, формируемые кредитной организацией (головной кредитной организацией банковской группы) в соответствии с пунктом 4.2 настоящего Положения.

4.2. Подразделение, ответственное за организацию управления операционным риском, формирует отчеты по операционному риску на ежеквартальной и ежегодной основе и обеспечивает ежедневное направление информации о событиях операционного риска или предоставление доступа к такой информации руководителю службы управления рисками.

4.2.1. Подразделение, ответственное за организацию управления операционным риском, ежедневно направляет руководителю службы управления рисками информацию о событиях операционного риска, зарегистрированных в базе событий за отчетную дату, предшествующую дате подготовке информации, об обстоятельствах их возникновения и их влиянии на соблюдение плановых (целевых) показателей уровня операционного риска, установленных в соответствии с пунктом 4.5 настоящего Положения, другую информацию (при наличии).

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

В случае если в кредитной организации (головной кредитной организации банковской группы) применяются программно-аппаратные средства, позволяющие обеспечить автоматизированное формирование информации из базы событий и ее направление в электронном виде руководителю службы управления рисками, а также организацию прямого доступа к базе событий (или другому информационному ресурсу) для самостоятельного просмотра (выгрузки) информации работниками службы управления рисками, кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок организации этих действий.

4.2.2. Подразделение, ответственное за организацию управления операционным риском, ежеквартально на определенную кредитной

организацией (головной кредитной организацией банковской группы) отчетную дату формирует и направляет руководителю службы управления рисками и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы) следующие отчеты:

об управлении операционным риском, содержащий информацию о событиях операционного риска и потерях кредитной организации (головной кредитной организации банковской группы, участников банковской группы) в разрезе элементов классификации событий операционного риска в соответствии с главой 3 настоящего Положения и отдельных видов операционного риска в соответствии с пунктом 1.4 настоящего Положения, содержащий информацию, указанную в подпункте 4.2.4 настоящего пункта, за исключением событий риска информационной безопасности, о результатах проведенных процедур управления операционным риском, в том числе о результатах процедуры количественной и качественной оценки уровня операционного риска, выбранных способах реагирования по результатам проведенной процедуры количественной и качественной оценки уровня операционного риска, результатах мониторинга операционного риска, результатах выполнения мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска;

о событиях риска информационной безопасности;

о фактических значениях контрольных показателей уровня операционного риска (включая контрольные показатели риска информационной безопасности в соответствии с подпунктом 1.2 пункта 1 приложения 1 к настоящему Положению).

4.2.3. Подразделение, ответственное за организацию управления операционным риском, ежегодно формирует и направляет руководителю службы управления рисками и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы) отчет об управлении операционным риском за год, содержащий

сведения о проведенных мероприятиях и работах, которые планируется провести в целях уменьшения негативного влияния риска операционного риска, а также информацию, указанную в абзацах втором – четвертом подпункта 4.2.2 настоящего пункта.

Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах порядок предоставления на рассмотрение совета директоров (наблюдательного совета) отчета об управлении операционным риском за год.

4.2.4. Информация о событиях операционного риска, включая события риска информационной безопасности, включается кредитной организацией (головной кредитной организацией банковской группы) в отчеты, указанные в подпункте 4.2.2 настоящего пункта, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, типов событий операционного риска и источников операционного риска отдельно по видам операционного риска и содержит в том числе следующие показатели:

общее количество событий операционного риска – количество всех событий операционного риска, которые были зафиксированы в кредитной организации (головной кредитной организации банковской группы) с начала года до отчетной даты и в отчетном периоде;

количество событий операционного риска в разрезе прямых и косвенных потерь с начала года до отчетной даты и в отчетном периоде;

количество событий операционного риска в разрезе потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, с начала года до отчетной даты и в отчетном периоде;

сумма прямых и сумма косвенных потерь от реализации событий операционного риска кредитной организации (головной кредитной организации банковской группы, включая потери от реализации операционного риска участников банковской группы) в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска, указанных в пункте 3.12 и подпункте 3.13.1

пункта 3.13 настоящего Положения, с начала года до отчетной даты и в отчетном периоде;

сумма потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, от реализации событий операционного риска кредитной организации (головной кредитной организации банковской группы в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска с начала года до отчетной даты и в отчетном периоде;

сумма прямых и сумма косвенных потерь, отнесенных к потерям, указанным в подпункте 3.12.8 пункта 3.12 и абзаце седьмом подпункта 3.13.1 пункта 3.13 настоящего Положения в части потерь на восстановление деятельности, в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска за отчетный период нарастающим итогом;

сумма прямых потерь от 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 и максимальная величина косвенных потерь от реализации одного события операционного риска с наибольшими потерями из тех событий операционного риска, которые были зафиксированы у кредитной организации (головной кредитной организации банковской группы), в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;

максимальная величина потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, от одного события операционного риска с наибольшими потерями из тех событий операционного риска, которые были зафиксированы у кредитной организации (головной кредитной организации банковской группы), в разрезе направлений

деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;

сумма прямых и сумма косвенных потерь от реализации пяти крупнейших (по сумме потерь) событий операционного риска из тех событий операционного риска, которые были зафиксированы у кредитной организации (головной кредитной организации банковской группы), в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;

сумма потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, от реализации пяти крупнейших (по сумме потерь) событий операционного риска из тех событий операционного риска, которые были зафиксированы у кредитной организации (головной кредитной организации банковской группы), в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, с начала года до отчетной даты и в отчетном периоде;

сумма возмещений по потерям за счет не связанных с кредитной организацией (головной кредитной организацией банковской группы) лиц, которые были отражены на балансовых счетах кредитной организации (головной кредитной организации банковской группы), в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска с начала года до отчетной даты и в отчетном периоде;

сумма возмещений по потерям за счет связанных с кредитной организацией (головной кредитной организацией банковской группы) юридических и физических лиц в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска с начала года до отчетной даты и в отчетном периоде;

сумма чистых (фактических) потерь, определяемых в соответствии с требованиями пункта 6.18 настоящего Положения, которая была отражена на

балансовых счетах кредитной организации (головной кредитной организации банковской группы) с начала года до отчетной даты и в отчетном периоде;

средняя величина прямых и средняя величина косвенных потерь от реализации одного события операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска за отчетный период;

среднеквадратичное отклонение (сигма) величины прямых потерь по группам событий операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и типов событий операционного риска за год (включается в отчет в случае, если количество событий операционного риска за отчетный период составляет более 100);

распределение потерь от реализации событий операционного риска по группам (менее 20 тысяч рублей, от 20 тысяч рублей до 100 тысяч рублей, от 100 тысяч рублей до 350 тысяч рублей, от 350 тысяч рублей до 700 тысяч рублей, от 700 тысяч рублей до 1 400 тысяч рублей, более 1 400 тысяч рублей).

4.2.5. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) рассматривает в установленные во внутренних документах кредитной организации (головной кредитной организации банковской группы) сроки (но не позднее двадцати рабочих дней со дня получения на рассмотрение) отчеты по операционным рискам кредитной организации (головной кредитной организации банковской группы) и дает поручения по разработке мероприятий, направленных на повышение качества системы управления операционным риском и уменьшение негативного влияния операционного риска, с указанием ответственных за реализацию мероприятий подразделений и сроков выполнения.

Отчеты по операционным рискам должны храниться кредитной организацией (головной кредитной организацией банковской группы) не менее десяти лет со дня рассмотрения коллегиальным исполнительным

органом кредитной организации (головной кредитной организации банковской группы).

4.3. Кредитная организация (головная кредитная организация банковской группы) дополнительно устанавливает во внутренних документах следующие требования.

4.3.1. Требования к информационной системе, обеспечивающей управление операционным риском и включающей автоматизацию ведения базы событий и процедур управления операционным риском.

Кредитная организация (головная кредитная организации банковской группы) организует информационный обмен информационной системы, обеспечивающей управление операционным риском, с другими информационными системами кредитной организации (головной кредитной организации банковской группы), позволяющими получать первичную информацию о сбоях систем и оборудования, об ошибках, отклонениях в процессах кредитной организации (головной кредитной организации банковской группы) и о реализации событий операционного риска, в зависимости от осуществляемых операций и (или) действующих процессов.

4.3.2. Требования к управлению модельным риском, включающие соблюдение следующих процедур:

выявление потенциальных ошибок в процессах разработки, проверки, адаптации, приемки, применения методик количественных и качественных моделей оценки активов (далее – модели оценки активов), включая оценку влияния этих ошибок на качество и прогнозную точность моделей оценки активов;

выявление недостоверности и неполноты данных, использованных при разработке и проверке моделей оценки активов, включая в том числе оценку влияния этих ошибок на качество моделей оценки активов, например, приводящих к невозможности определения значения одного или нескольких входных параметров модели оценки активов или существенных факторов, использованных в модели оценки активов;

контроль за разработкой моделей оценки активов, проверка правильности применения методик и технологий моделирования, в том числе правильности постановки задачи на разработку, принимаемых допущений, использования в моделях оценки активов всех существенных факторов, оценки прогнозной точности моделей оценки активов, контроль за соответствием моделей оценки активов условиям внешней среды и внешним и внутренним факторам их применения;

выявление ошибок в процессах регистрации, учета и отчетности о результатах разработки и применения моделей оценки активов;

контроль за полнотой документации о разработке моделей оценки активов и ее применением;

контроль за своевременностью калибровки моделей оценки активов, связанной с изменением внешних и внутренних факторов их применения и поступлением новых данных, свидетельствующих о снижении качества моделей оценки активов и их прогнозной точности;

валидация моделей оценки активов (подразделением кредитной организации (головной кредитной организации банковской группы) и (или) внешними экспертами);

контроль качества валидации моделей оценки активов, в том числе корректности применения валидационных тестов и критериев, включая контроль за правильностью интерпретации результатов валидации и реагирования на эти результаты;

контроль за внедрением моделей оценки активов в промышленную эксплуатацию, в том числе за имплементацией программного кода в автоматизированные системы кредитной организации (головной кредитной организации банковской группы);

выявление ошибок в интерпретации результатов моделей оценки активов для принятия управленческих решений и бизнес-решений в кредитной организации (головной кредитной организации банковской группы), в том

числе связанных с использованием моделей оценки активов в предметных областях, для которых они не разрабатывались и не валидировались.

4.4. Уполномоченное подразделение кредитной организации (головной кредитной организации банковской группы) в соответствии с порядком, указанном в подпункте 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;

корректности определения вида и величины потерь от реализации событий операционного риска;

соблюдения установленных кредитной организацией (головной кредитной организацией банковской группы) в политике управления операционным риском и в других внутренних документах требований и процедур управления операционным риском;

корректности проведенных оценок величины потерь от реализации событий операционного риска;

комплекса мероприятий, разрабатываемого в соответствии с подпунктом 4.1.5 пункта 4.1 настоящего Положения;

эффективности мер, направленных на уменьшение негативного влияния операционного риска;

соблюдения других требований настоящего Положения.

4.5. Кредитная организация (головная кредитная организация банковской группы) в целях осуществления контроля за объемом операционного риска, принятым в кредитной организации (головной кредитной организацией банковской группы), в соответствии с пунктом 3.4 Указания Банка России № 3624-У разрабатывает и устанавливает плановые (целевые) показатели уровня операционного риска в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, которые формируются кредитной организацией (головной кредитной организацией

банковской группы) на основе следующих данных, характеризующих объемы операций, подверженных операционному риску за определенный период (день, неделя, месяц, квартал, полугодие, девять месяцев, год):

количество сделок, операций, транзакций;

объем сделок, операций, транзакций в денежном выражении в рублях;

количество платежей, осуществленных через корреспондентский счет кредитной организации (головной кредитной организации банковской группы) и другие корреспондентские счета;

доход за год для целей расчета капитала на покрытие операционного риска;

обороты по счетам бухгалтерского учета;

другие данные.

Кредитная организация (головная кредитная организация банковской группы) соотносит данные, характеризующие объем операций, с зарегистрированными в базе событий потерями и определяет показатели уровня операционного риска, порядок соблюдения которых устанавливается кредитной организацией (головной кредитной организацией банковской группы) во внутренних документах.

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 осуществляемых операций и (или) действующих процессов, изменяющихся внешних факторов, результатов процедур управления операционным риском, результатов оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, изменений в стратегии управления рисками и капиталом и направляет результаты анализа на рассмотрение коллегиальным исполнительным органом кредитной организации (головной кредитной организации банковской группы) для принятия решения о необходимости внесения изменений во внутренние

документы, указанные в подпунктах 4.1.2 и 4.1.3 пункта 4.1 настоящего Положения.

Глава 5. **Система контрольных показателей уровня операционного риска**

5.1. В целях контроля за уровнем операционного риска кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах на плановый годовой период в соответствии с приложением 1 к настоящему Положению контрольные показатели уровня операционного риска, а также устанавливает целевые значения этих показателей: значение показателя, при нарушении которого проводится ежедневный мониторинг значений показателя и реализация мер, 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 во внутренних документах кредитной организации (головной кредитной организации банковской группы) в соответствии с пунктом 5.4 настоящего Положения (далее – контрольное значение).

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

утверждает сигнальные и контрольные значения контрольных показателей уровня операционного риска на плановый годовой период как в целом по кредитной организации (головной кредитной организации банковской группы), так и в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, и подразделений, ответственных за осуществление операций и сделок и за результаты процесса, которые ежегодно подлежат пересмотру и актуализации кредитной организацией (головной кредитной организацией банковской группы) в рамках оценки

соответствия процедур управления рисками текущей ситуации в кредитной организации, проводимой в соответствии с абзацем первым 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 контрольных показателей уровня операционного риска;

обеспечивает реагирование кредитной организации (головной кредитной организации банковской группы) в случае превышения сигнальных и контрольных значений контрольных показателей уровня операционного риска.

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

В случае если период ведения базы событий составляет менее десяти лет, кредитная организация (головная кредитная организация банковской группы) определяет методику учета недостающих данных во внутренних документах и производит расчет на основе фактически имеющегося периода наблюдений с последующим добавлением данных за новые годы по мере их накопления вплоть до достижения десяти лет.

Подразделение, ответственное за организацию управления операционным риском, оформляет расчет и обоснование сигнальных и контрольных значений контрольных показателей уровня операционного риска в виде заключения и включает его в состав материалов, направляемых им на рассмотрение коллегиальным исполнительным органом кредитной

организации (головной кредитной организации банковской группы) при утверждении (пересмотре) политики управления операционным риском.

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

Глава 6. **Ведение базы событий**

6.1. Кредитная организация (головная кредитная организация банковской группы) осуществляет ведение на постоянной основе базы событий.

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

6.3. Головная кредитная организация банковской группы определяет во внутренних документах порядок ведения базы событий консолидировано по банковской группе с учетом потерь от реализации операционного риска у участников банковской группы. В случае раздельного ведения базы событий дочерние кредитные организации на ежемесячной основе предоставляют данные о событиях операционного риска и потерях в головную кредитную

организацию банковской группы в целях расчета объема капитала банковской группы, выделяемого на покрытие потерь от реализации операционного риска, и соблюдения ВПОДК банковской группы.

В случае если база событий ведется головной кредитной организацией банковской группы раздельно с дочерними кредитными организациями, дочерние кредитные организации определяют во внутренних документах порядок ведения базы событий, который согласовывают с головной кредитной организацией банковской группы.

В случае если дочерние кредитные организации ведут учет событий операционного риска по элементам классификации, отличным от предусмотренных главой 3 настоящего Положения, например, в случае нахождения дочерней кредитной организации вне юрисдикции Российской Федерации, головная кредитная организация банковской группы устанавливает во внутренних документах правила соотнесения классификации событий операционного риска дочерних кредитных организаций, ведущих учет событий операционного риска по другим элементам классификации, с требованиями главы 3 настоящего Положения и определяет порядок предоставления отчетов дочерних кредитных организаций с учетом правил соотнесения классификации.

Головная кредитная организация банковской группы в случае необходимости определяет во внутренних документах дополнительные отчеты участников банковской группы по операционному риску, направляемые в головную кредитную организацию банковской группы.

6.4. Данные о событиях операционного риска и потерях от реализации событий операционного риска должны охватывать всю деятельность кредитной организации (головной кредитной организации банковской группы), все подразделения, организационные, информационные и технологические системы и регионы присутствия кредитной организации (головной кредитной организации 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. Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах величину прямых и непрямых потерь от реализации события операционного риска, при котором кредитная организация (головная кредитная организация банковской группы) регистрирует событие операционного риска в базе событий (далее – порог регистрации).

Порог регистрации устанавливается кредитной организацией (головной кредитной организацией банковской группы) в зависимости от величины потерь и типа событий операционного риска:

для событий операционного риска, относящихся к типам событий операционного риска, указанным в подпунктах 3.6.1 и 3.6.2 пункта 3.6 настоящего Положения, порог регистрации в базе событий не устанавливается;

для событий операционного риска, потери по которым относятся к указанным в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, порог регистрации в базе событий не устанавливается;

для других типов событий операционного риска, потери по которым относятся к прямым и непрямым потерям, за исключением потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, порог регистрации в базе событий составляет не более 20 тысяч рублей.

Дочерняя кредитная организация банковской группы, созданная в соответствии с правом иностранного государства, регулирование деятельности которой осуществляется центральным банком и (или) иным органом надзора иностранного государства, в функции которого входят банковский надзор и надзор за финансовым рынком, соблюдает порог регистрации событий операционного риска в соответствии с требованиями, установленными центральным банком и (или) иным органом иностранного

государства, в юрисдикции которых находится данная дочерняя кредитная организация банковской группы. В случае если центральным банком и (или) иным органом надзора иностранного государства, в функции которого входят банковский надзор и надзор за финансовым рынком, в юрисдикции которых находится данная дочерняя кредитная организация банковской группы, не установлены требования к порогу регистрации событий операционного риска в базе событий, головная кредитная организация банковской группы устанавливает во внутренних документах для данных дочерних кредитных организаций порог регистрации событий операционного риска в базе событий, предусмотренный настоящим пунктом.

В случае если событие операционного риска привело только к качественным потерям, оценка значимости которых в соответствии с абзацем двенадцатым подпункта 3.13.2 пункта 3.13 настоящего Положения соотносится с уровнем «средние» или «низкие», кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах требования к регистрации таких событий операционного риска в базе событий.

Основанием для регистрации событий, повлекших потери, указанные в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, является результат рассмотрения кредитной организацией (головной кредитной организацией банковской группы) обращений клиентов, контрагентов, работников и третьих лиц в установленном во внутренних документах порядке.

6.6. База событий кредитной организации (головной кредитной организации банковской группы, кредитных организаций 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 операционного риска объединены в группу), определяемой в соответствии с пунктом 6.12 настоящего Положения;

дату, когда событие операционного риска было зарегистрировано в базе событий (дата регистрации);

время регистрации события операционного риска в базе событий в случае программно-аппаратной фиксации событий операционного риска;

дату, когда событие операционного риска произошло или впервые началось (дата реализации);

время, когда событие операционного риска произошло или впервые началось, в случае программно-аппаратной фиксации событий риска информационной безопасности и других событий операционного риска;

дату (и время в случае, если характер события операционного риска это предусматривает), когда кредитной организации (головной кредитной организации банковской группы) стало известно о событии операционного риска (дата выявления);

дату (и время для событий риска информационной безопасности) окончания события операционного риска (дата окончания события) в случае, если наличие такой информации определяется характером события операционного риска;

статус события операционного риска (в том числе «оценка потерь от реализации события операционного риска завершена» и «оценка потерь от реализации события операционного риска не завершена»). При этом кредитная организация (головная кредитная организация банковской группы) определяет виды статусов события операционного риска;

подразделение, в котором произошло событие операционного риска;

подразделение, выявившее событие операционного риска;

описание события операционного риска (детализированное описание события операционного риска, включающее ответы на вопросы: в чем

заключается событие операционного риска, каким образом оно было обнаружено, что явилось его причиной (причинами);

категорию источника операционного риска в соответствии с пунктом 3.3 настоящего Положения;

значимые источники операционного риска, которые повлияли на реализацию события операционного риска, согласно письменному обоснованию работника кредитной организации (головной кредитной организации банковской группы) с указанием долей их влияния в отношении события операционного риска, установленных в соответствии с внутренними документами кредитной организации (головной кредитной организации банковской группы);

тип события операционного риска в соответствии с пунктом 3.6 настоящего Положения;

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

связь с другими видами риска (кредитным, рыночным, риском ликвидности, стратегическим, риском потери деловой репутации и другими) при наличии такой связи. При этом кредитная организация (головная кредитная организация банковской группы) указывает, является ли другой вид риска источником или следствием события операционного риска;

идентификатор связанного события операционного риска в случае, если такая связь установлена. При этом кредитная организация (головная кредитная организация банковской группы) указывает, является ли событие операционного риска источником или следствием другого события операционного риска;

дополнительную классификацию типа события операционного риска в зависимости от вида риска;

направление деятельности в соответствии с пунктом 3.9 настоящего Положения;

процесс согласно перечню процессов, определенному во внутренних документах кредитной организации (головной кредитной организации банковской группы);

этап процесса согласно определенным в кредитной организации (головной кредитной организации банковской группы) правилам описания процессов (при наличии);

информационную систему (в случае, если информационная система задействована при выполнении этапа процесса);

меры, направленные на уменьшение негативного влияния операционного риска.

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 3.11 настоящего Положения;

признак связи потери с другим видом риска (при наличии такой связи), который не будет включаться кредитной организацией (головной кредитной организацией банковской группы) в состав валовых потерь, определяемых в соответствии с пунктом 6.7 настоящего Положения;

величину потери от реализации события операционного риска в рублях, определяемую в соответствии с внутренними документами кредитной организации (головной кредитной организации банковской группы) (например, в случае прямых потерь – сумма бухгалтерской записи по счетам бухгалтерского учета, в случае непрямых потерь – оценочное значение, при этом для событий операционного риска, связанных с кредитным риском, отсутствует необходимость ежедневного пересмотра суммы основного долга (или остатка основного долга) и процентов по нему в базе событий при условии отражения данных в базе событий на дату возникновения события операционного риска и на ежеквартальной основе);

дату учета потери, то есть дату отражения потери от реализации события операционного риска на счетах бухгалтерского учета (например, для событий

правового риска датой учета потерь являются дата создания (изменения) резерва в соответствии с абзацем пятым подпункта 3.12.6 пункта 3.12 настоящего Положения и даты отражения в бухгалтерском учете других связанных с этим обстоятельством расходов; для событий операционного риска, связанных с кредитным риском, датой учета потерь является дата создания (изменения) резерва в соответствии с абзацем четвертым подпункта 3.12.1 пункта 3.12 настоящего Положения);

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

экспертную оценку качественной потери, определяемой в соответствии с подпунктом 3.13.2 пункта 3.13 настоящего Положения, в случае регистрации наличия качественной потери для события операционного риска, в результате которого возникла данная потеря;

обоснование величины потери (для косвенных потерь размером менее 100 тысяч рублей обоснование не заполняется) или причину, по которой потери не возникли. Формат обоснования величины потери кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах самостоятельно;

агрегированную сумму валовых потерь в рублях;

агрегированную сумму прямых потерь в рублях;

агрегированную сумму косвенных потерь в рублях;

сумму потерь, указанных в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, в рублях.

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

мероприятия, осуществленные кредитной организацией (головной кредитной организацией банковской группы) в целях получения возмещения по понесенным потерям от реализации события операционного риска;

вид возмещения в соответствии с пунктом 6.15 настоящего Положения;

признак связи возмещения с видом потерь от реализации конкретного события операционного риска, определяемым в соответствии с пунктом 3.11 настоящего Положения;

сумму возмещения в рублях;

дату отражения возмещения на счетах бухгалтерского учета;

информацию о бухгалтерской записи суммы возмещения;

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

сумму чистых (фактических) потерь, определяемых в соответствии с пунктом 6.18 настоящего Положения.

В случае если сумма потерь и возмещений отражается кредитной организацией (головной кредитной организацией банковской группы) в иностранной валюте, пересчет в рубли осуществляется кредитной организацией (головной кредитной организацией банковской группы) в базе событий по официальному курсу иностранной валюты по отношению к рублю, установленному Банком России в соответствии с пунктом 15 статьи 4 Федерального закона № 86-ФЗ (Собрание законодательства Российской Федерации, 2002, № 28, ст. 2790; 2019, № 29, ст. 3857) (далее – курс иностранной валюты, установленный Банком России), на дату отражения в бухгалтерском учете кредитной организации (головной кредитной организацией банковской группы).

В случае если сумма возмещений в рублях, рассчитанная в соответствии с курсом иностранной валюты, установленным Банком России, превышает

сумму потерь в рублях, в базе событий должна быть отражена сумма потерь в рублях.

В случае если кредитная организация (головная кредитная организация банковской группы) использует дополнительные поля базы событий, кредитная организация (головная кредитная организация банковской группы) определяет их во внутренних документах.

6.7. Кредитная организация (головная кредитная организация банковской группы) ежемесячно на отчетную дату определяет величину валовых потерь от реализации событий операционного риска со статусом «оценка потерь от реализации события операционного риска не завершена» начиная от даты 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 валовых потерь кредитной организацией (головной кредитной организацией банковской группы) включаются потери от реализации событий операционного риска, статус которых был переведен в статус «оценка потерь от реализации события операционного риска завершена», в течение отчетного месяца.

Головная кредитная организация банковской группы для целей расчета величины валовых потерь по банковской группе осуществляет перерасчет величины валовых потерь и последующих возмещений от событий операционного риска, произошедших у иностранных дочерних кредитных организаций, 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 (за исключением событий операционного риска, связанных с реализацией кредитного риска).

6.7.1. В расчет величины валовых потерь кредитной организацией (головной кредитной организацией банковской группы) включаются:

сумма прямых потерь от реализации события операционного риска, определяемых в соответствии с пунктом 3.12 настоящего Положения, включая обесценение, списание активов, отраженных на счетах бухгалтерского учета кредитной организации (головной кредитной организации банковской группы);

корректировка стоимости прямых потерь, не отраженных в бухгалтерском учете в течение текущего календарного года, связанных с перерасчетом величины прямых потерь от реализации события операционного риска прошлого периода, в случае, если отражение в бухгалтерском учете потерь длится более одного календарного года (распределенные во времени потери). При этом в случае такой корректировки потери рассчитываются кредитной организацией (головной кредитной организацией банковской группы) в корреспонденции со счетами расходов текущего года;

сумма прямых потерь по событиям операционного риска, которые вызывают искажение финансовой отчетности кредитной организации (головной кредитной организации банковской группы) за определенный отчетный период (календарный год), но которые могут быть полностью скорректированы в дальнейшем (например, при завершении расчетов, создании исправительных бухгалтерских записей и переоценке справедливой стоимости финансовых инструментов, при определении временных потерь).

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок учета величины валовых потерь, позволяющий точно определять уровень операционного риска, в том числе для целей расчета показателя, указанного в абзаце седьмом подпункта 1.1.1 пункта 1 приложения 1 к настоящему Положению.

6.7.2. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок идентификации потерь и возмещений в разрезе всех событий операционного риска, повлекших потери, с указанием дат учета, сумм и реквизитов бухгалтерских записей.

6.7.3. В валовые потери кредитной организацией (головной кредитной организацией банковской группы) не включаются:

расходы кредитной организации (головной кредитной организации банковской группы) по договорам на поддержание и регулярное обслуживание систем инженерно-технического обеспечения;

внутренние и внешние расходы кредитной организации (головной кредитной организации банковской группы), направленные на улучшение деятельности после завершения оценки потерь от реализации операционного риска (модернизация, совершенствование, мероприятия по предотвращению риска, улучшению качества процессов, оценке рисков и расширению функционала по управлению операционным риском);

выплата страховых премий;

расходы, связанные с доначислением резервов на возможные потери по ссудам, ссудной и приравненной к ней задолженности, формируемых в соответствии с пунктом 1.1 Положения Банка России № 590-П, по событиям операционного риска, повлекшим реализацию кредитного риска по конкретным ссудам, ссудной и приравненной к ней задолженности, за исключением случаев, когда указанные расходы возникли в результате реализации события операционного риска, тип которого указан в подпункте 3.6.1 пункта 3.6 настоящего Положения.

6.8. По одному событию операционного риска кредитной организацией (головной кредитной организацией банковской группы) выявляются и учитываются в базе событий все виды произошедших потерь. Каждая потеря отражается кредитной организацией (головной кредитной организацией банковской группы) в базе событий отдельной записью с указанием идентификатора записи потери и номера бухгалтерской записи (идентификатора бухгалтерской записи), даты учета потери и с пометкой о связи с другим видом риска.

Кредитная организация (головная кредитная организация банковской группы) указывает перечень всех бухгалтерских записей одного вида потерь

от реализации события операционного риска при указании в базе событий информации, приведенной в абзаце тринадцатом пункта 6.6 настоящего Положения, или в виде вложения со списком всех бухгалтерских записей в разбивке по суммам.

6.9. Кредитная организация (головная кредитная организация банковской группы) ведет учет потерь от реализации событий всех видов операционного риска, событий операционного риска, связанных с потерями, указанными в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения, и событий других нефинансовых рисков в составе общей базы событий либо раздельно. При этом кредитная организация (головная кредитная организация банковской группы) устанавливает единый подход к идентификации, оценке и классификации в соответствии с главами 2 и 3 настоящего Положения, исключающий дублирование и пропуски информации, в целях определения количественных контрольных показателей уровня операционного риска, указанных в приложении 1 к настоящему Положению.

6.10. В случае если кредитная организация (головная кредитная организация банковской группы) ведет базу событий отдельных видов операционного риска, событий регуляторного риска и (или) событий других нефинансовых рисков раздельно, кредитная организация (головная кредитная организация банковской группы) ежемесячно на отчетную дату включает события регуляторного риска и других нефинансовых рисков с прямыми потерями, связанными с реализацией операционного риска, в состав базы событий 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.

6.12. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах специальные критерии для определения данных о потерях, вызванных единичными событиями операционного риска, и о потерях, вызванных однородными событиями операционного риска, произошедшими в течение установленного во внутренних документах периода времени (группа событий).

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах критерии однородности событий операционного риска для целей их группировки (например, события операционного риска объединяются кредитной организацией (головной кредитной организацией банковской группы) в одну группу в случае, если у них одинаковый источник операционного риска, один и тот же процесс или этап процесса, тип события операционного риска, а период времени возникновения составил не более 48 часов). Группировка событий операционного риска должна быть предметом оценки, проводимой уполномоченным подразделением.

6.13. Возмещения потерь отражаются в группе полей базы событий, содержащей информацию о полученном возмещении понесенных потерь, по каждому событию операционного риска. Каждое возмещение потерь должно быть связано с регистрацией в бухгалтерском учете компенсации потери от реализации события операционного риска, отражено на счетах бухгалтерского учета в виде бухгалтерской записи по счетам доходов (прибылей), обратной бухгалтерской записи, другой бухгалтерской записи с указанием номера бухгалтерской записи (идентификатора бухгалтерской записи), даты записи.

6.14. Кредитная организация (головная кредитная организация банковской группы) отражает в базе событий все возмещения одного вида по каждой потере от реализации события операционного риска при указании в базе событий информации, приведенной в абзаце тринадцатом пункта 6.6 настоящего Положения, или в виде вложения со списком всех бухгалтерских записей в разбивке по суммам.

6.15. Виды возмещений потерь:

возмещения, полученные в судебном порядке;

возмещения, полученные во внесудебном порядке по соглашению сторон;

страховые выплаты от одной или нескольких страховых организаций;

возмещения, полученные от третьих лиц;

возмещения от работников кредитной организации (головной кредитной организации банковской группы, участника банковской группы);

возмещения, полученные из других источников;

восстановление резерва на возможные потери по ссудам, ссудной и приравненной к ней задолженности в соответствии с Положением Банка России № 590-П и Указанием Банка России № 1584-У;

восстановление резерва по прочим потерям и обязательствам некредитного характера в соответствии с Положением Банка России № 611-П.

6.16. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок контроля за своевременностью отражения возмещения потерь от реализации событий операционного риска.

6.17. Кредитная организация (головная кредитная организация банковской группы) должна учитывать в базе событий отдельно валовые потери и чистые (фактические) потери, определяемые в соответствии с пунктом 6.18 настоящего Положения. Возмещение используется кредитной организацией (головной кредитной организацией банковской группы) для уменьшения потерь только после того, как платеж получен кредитной организацией (головной кредитной организацией банковской группы) и отражен на счетах бухгалтерского учета. Дебиторская задолженность не является возмещением.

В случае поступления возмещения от третьего лица в базе событий кредитная организация (головная кредитная организация банковской группы) указывает наименование третьего лица и его характеристики (например,

страховая организация, контрагент, признак связи с кредитной организацией или банковской группой).

К зачету сумм возмещения кредитной организацией (головной кредитной организации банковской группы) не принимаются следующие виды возмещений:

возмещения, полученные от страховых организаций, входящих в банковскую группу (за исключением случая, когда возмещение от страховой организации, входящей в банковскую группу, получено в рамках перестрахования рисков от страховых брокеров, не входящих в банковскую группу);

возмещения от связанных с кредитной организацией (головной кредитной организации банковской группы, участниками банковской группы) лиц, акционеров, бенефициаров;

возмещения от других физических и юридических лиц, способных оказать влияние на деятельность кредитной организации (головной кредитной организации банковской группы, участников банковской группы).

Проверка достоверности, полноты и своевременности учета возмещений должна включаться кредитной организацией (головной кредитной организацией банковской группы) в программу оценки эффективности функционирования системы управления операционным риском, проводимой уполномоченным подразделением.

6.18. Чистые (фактические) потери от реализации события операционного риска определяются как потери за вычетом суммы возмещения с учетом требований пункта 6.17 настоящего Положения.

6.19. В случае корректировки значения потерь и возмещений в базе событий предыдущее значение потерь кредитной организацией (головной кредитной организацией банковской группы) не исправляется, а добавляется новая информация с новым значением (должна быть обеспечена сохранность предыдущих значений).

Информация о событиях операционного риска в базе событий подлежит ежегодной независимой оценке, проводимой уполномоченным подразделением.

6.20. Кредитная организация (головная кредитная организация банковской группы) обеспечивает сохранность всех записей в базе событий. Внесение изменений и дополнений в информацию базы событий фиксируется кредитной организацией (головной кредитной организацией банковской группы) с указанием фамилии, имени, отчества (последнее при наличии) работника, сделавшего исправление, даты и основания исправления. Корректность исправления записи в соответствии с указанным основанием подлежит верификации в соответствии с внутренними документами кредитной организации (головной кредитной организации банковской группы).

6.21. Кредитная организация (головная кредитная организация банковской группы) устанавливает перечень должностей работников кредитной организации (головной кредитной организации банковской группы) с возложением полномочий и персональной ответственности на лиц, их замещающих, за несоблюдение требований внутренних документов по ведению базы событий, в том числе указывает во внутренних документах:

перечень должностей работников, ответственных за ведение базы событий;

перечень должностей работников, предоставляющих информацию для базы событий;

перечень должностей работников, определяющих потери от реализации событий операционного риска, занесенные в базу событий;

перечень должностей работников, ответственных за проверку полноты информации в базе событий и сверку счетов бухгалтерского учета с информацией, отраженной в базе событий.

Глава 7. **Управление риском информационной безопасности**

7.1. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок управления риском информационной безопасности.

7.2. Риск информационной безопасности включает в себя:

риск преднамеренных действий со стороны работников кредитной организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа (далее – киберриск);

другие виды риска информационной безопасности, связанных с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры.

7.3. Инциденты, приведшие к фактической реализации риска информационной безопасности, в том числе киберриска, обусловленные источниками риска информационной безопасности, в том числе инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных в соответствии с Положением 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», зарегистрированным

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), и Положением Банка России от 17 апреля 2019 года № 683-П «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента», зарегистрированным Министерством юстиции Российской Федерации 16 мая 2019 года № 54637 (далее – Положение Банка России № 683-П) (далее – инциденты защиты информации), вследствие которых возникли прямые и непрямые потери кредитной организации (головной кредитной организации банковской группы) (далее – событие риска информационной безопасности), фиксируются кредитной организацией (головной кредитной организацией банковской группы) в базе событий с присвоением вида операционного риска в соответствии с абзацем семнадцатым пункта 6.6 настоящего Положения.

Негативное влияние риска информационной безопасности должно определяться в виде потерь, приведенных в пункте 3.11 настоящего Положения и пункте 4 приложения 5 к настоящему Положению.

7.4. Кредитная организация (головная кредитная организация банковской группы) классифицирует события риска информационной безопасности по источникам операционного риска в соответствии с пунктом 3.3 настоящего Положения, а также по уязвимостям информационных систем и их компонентов как источникам последующих уровней классификации источников событий операционного риска в соответствии с пунктом 3.4 настоящего Положения, обусловленным недостатками процессов обеспечения защиты информации, способствующими реализации угрозы безопасности информации

(совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации).

7.5. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок ведения базы событий риска информационной безопасности (как в общей базе событий, так и в отдельной базе событий риска информационной безопасности). В случае если кредитная организация (головная кредитная организация банковской группы) ведет отдельную базу событий риска информационной безопасности, подразделению (работникам), ответственному (ответственным) за организацию и контроль обеспечения защиты информации (далее – служба информационной безопасности), необходимо соблюдать требования к классификации событий риска информационной безопасности в соответствии с пунктами 3.3–3.15 настоящего Положения и требования к ведению базы событий в соответствии с пунктами 6.6–6.21 настоящего Положения.

7.6. Кредитная организация (головная кредитная организация банковской группы) обеспечивает выявление, регистрацию и учет всех событий риска информационной безопасности с определением всех элементов классификации в соответствии с главами 2, 3 и 6 настоящего Положения, приложениями 4 и 5 к настоящему Положению, определяет суммы потерь в разрезе видов потерь в соответствии с пунктом 3.11 настоящего Положения и пунктом 4 приложения 5 к настоящему Положению с распределением по датам отражения в бухгалтерском учете, с раздельным учетом поступивших возмещений.

7.7. Кредитная организация (головная кредитная организация банковской группы) в целях управления риском информационной безопасности определяет во внутренних документах порядок функционирования системы информационной безопасности и обеспечивает его выполнение, в том числе:

политику информационной безопасности;

выявление и идентификацию риска информационной безопасности, а также его оценку;

участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа кредитной организации (головной кредитной организации банковской группы) в решении вопросов управления риском информационной безопасности;

распределение функций и ответственности коллегиального исполнительного органа и работников кредитной организации (головной кредитной организации банковской группы), в том числе исключающее конфликт интересов в рамках организационной структуры обеспечения информационной безопасности, а также предполагающее определение должностного лица (лица, его замещающего), ответственного за функционирование системы обеспечения информационной безопасности (с прямым подчинением лицу, осуществляющему функции единоличного исполнительного органа кредитной организации (головной кредитной организации банковской группы), или его заместителю) и не участвующего в совершении операций, сделок, организации бухгалтерского и управленческого учета, обеспечении функционирования информационных систем;

защиту от угроз безопасности информации, включая обеспечение защиты информации, управление риском информационной безопасности при передаче внешним контрагентам выполнения отдельных функций кредитной организации (головной кредитной организации банковской группы) и (или) использовании внешних информационных систем в рамках реализации направлений деятельности, в том числе в разрезе составляющих их процессов, кредитной организации (головной кредитной организации банковской группы), а также операционную надежность, в том числе на этапах жизненного цикла информационных систем кредитной организации (головной кредитной организации банковской группы), в части управления

изменениями, конфигурациями (настраиваемыми параметрами) и уязвимостями объектов информационной инфраструктуры;

выявление событий риска информационной безопасности, включая обнаружение компьютерных атак, рассмотрение обращений клиентов, контрагентов, работников и третьих лиц, связанных с нарушением информационной безопасности, выявление и регистрацию инцидентов защиты информации, выявление уязвимостей и фактов компрометации объектов информационной инфраструктуры;

порядок реагирования на выявленные события риска информационной безопасности и восстановления деятельности кредитной организации (головной кредитной организации банковской группы) в случае реализации таких событий, включая порядок взаимодействия кредитной организации (головной кредитной организации банковской группы) с клиентами и третьими лицами, в том числе в случае получения уведомлений об осуществлении переводов денежных средств без согласия клиентов;

обмен информацией о событиях риска информационной безопасности, в том числе об инцидентах защиты информации, и предоставление данных в Банк России в соответствии с требованиями пункта 8 Положения Банка России № 683-П;

организацию ресурсного (кадрового и финансового) обеспечения, включая установление требований к квалификации работников кредитной организации (головной кредитной организации банковской группы), в том числе должностного лица (лица, его замещающего), ответственного за функционирование системы обеспечения информационной безопасности;

повышение осведомленности, обучение и развитие навыков работников кредитной организации (головной кредитной организации банковской группы) в области противодействия угрозам безопасности информации;

установление и реализацию программ контроля, в том числе программ аудита;

соответствие фактических значений контрольных показателей уровня риска информационной безопасности принятым в кредитной организации (головной кредитной организации банковской группы) значениям;

планирование, реализацию, контроль и совершенствование комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности, в том числе в соответствии с реализуемыми уровнями защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями подпункта 3.1 пункта 3 Положения Банка России № 683-П;

выполнение требований к обеспечению защиты информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, в соответствии с пунктом 5 Положения Банка России № 683-П;

процессы применения прикладного программного обеспечения автоматизированных систем и приложений, соответствующих требованиям пункта 4 Положения Банка России № 683-П;

ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры в соответствии с подпунктом 3.2 пункта 3 Положения Банка России № 683-П;

независимую оценку соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями пункта 9 Положения Банка России № 683-П.

7.8. В политике информационной безопасности кредитная организация (головная кредитная организация банковской группы) в целях управления риском информационной безопасности определяет:

функции и ответственность коллегиального исполнительного органа и работников кредитной организации (головной кредитной организации

банковской группы) в рамках управления риском информационной безопасности;

основные принципы функционирования системы обеспечения информационной безопасности;

сигнальные и контрольные значения контрольных показателей уровня риска информационной безопасности;

основные принципы организации контроля за функционированием системы обеспечения информационной безопасности;

требования к созданию ресурсных (кадровых и финансовых) условий системы обеспечения информационной безопасности;

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

Политика информационной безопасности должна утверждаться коллегиальным исполнительным органом кредитной организации (головной кредитной организации банковской группы).

Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) несет ответственность за соблюдение требований политики информационной безопасности.

7.9. Кредитная организация (головная кредитная организация банковской группы) с учетом требований, указанных в главе 9 настоящего Положения, определяет выполнение службой информационной безопасности или отдельным структурным подразделением, ответственным за обеспечение информационной безопасности, следующих функций.

7.9.1. В целях обеспечения информационной безопасности:

разработка политики информационной безопасности;

контроль осуществления работниками кредитной организации (головной кредитной организации банковской группы) мероприятий в области обеспечения информационной безопасности и защиты информации и

выполнения других задач, возложенных на них внутренними документами кредитной организации (головной кредитной организации банковской группы);

осуществление планирования и контроля процессов обеспечения информационной безопасности в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

разработка предложений по совершенствованию процессов обеспечения информационной безопасности, в том числе в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

составление отчетов по обеспечению информационной безопасности и направление их должностному лицу, ответственному за обеспечение информационной безопасности;

осуществление других функций, связанных с обеспечением информационной безопасности, предусмотренных внутренними документами кредитной организации (головной кредитной организации банковской группы).

7.9.2. В целях управления риском информационной безопасности:

соблюдение процедур управления операционным риском, установленных в подпунктах 2.1.1, 2.1.2 и 2.1.7 пункта 2.1 настоящего Положения, в части идентификации, сбора и регистрации информации о событиях риска информационной безопасности и потерях в базе событий, мониторинга риска информационной безопасности, в том числе на основе информации, предоставляемой центрами компетенций, ответственными за сбор информации о событиях операционного риска;

ведение базы событий риска информационной безопасности;

участие в реализации процессов в рамках комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности;

оценка эффективности управления риском информационной безопасности;

составление отчетов по событиям риска информационной безопасности и направление их в службу управления рисками и должностному лицу, ответственному за обеспечение информационной безопасности, а при его отсутствии – коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы);

осуществление мониторинга сигнальных и контрольных значений контрольных показателей уровня риска информационной безопасности, определенных в соответствии с подпунктом 1.2 пункта 1 приложения 1 к настоящему Положению;

участие в разработке внутренних документов в области управления риском информационной безопасности;

информирование работников кредитной организации (головной кредитной организации банковской группы) по вопросам, связанным с управлением риском информационной безопасности;

осуществление других функций, связанных с управлением риском информационной безопасности, предусмотренных внутренними документами кредитной организации (головной кредитной организации банковской группы).

7.10. Служба информационной безопасности формирует следующие специализированные отчеты по рискам информационной безопасности, направляемые на рассмотрение коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы), в дополнение к отчетам, формируемым подразделением,

ответственным за организацию управления операционным риском в соответствии с пунктом 4.2 настоящего Положения:

отчеты в соответствии с подпунктом 2.15.3 пункта 2.15 Положения Банка России № 382-П;

сводные отчеты, направляемые должностному лицу, ответственному за обеспечение информационной безопасности, и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы).

Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах порядок и сроки предоставления данных отчетов.

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

Глава 8. **Управление риском информационных систем**

8.1. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок управления риском информационных систем, включающий мероприятия и процедуры по обеспечению требований к непрерывности и качеству функционирования информационных систем и обеспечению качества данных в информационных системах.

8.2. В целях управления риском информационных систем кредитная организация (головная кредитная организация банковской группы) во внутренних документах определяет политику информационных систем как взаимосвязанной совокупности технических и программных средств, других объектов информационной инфраструктуры, содержащейся в базах данных информации и обеспечивающих ее обработку технологий в рамках реализации мероприятий поддержки и обеспечения непрерывности функционирования

процессов кредитной организации (головной кредитной организации банковской группы) и обеспечивает ее соблюдение.

8.3. В политике информационных систем кредитная организация (головная кредитная организация банковской группы) в целях управления риском информационных систем определяет:

функции и полномочия подразделения (подразделений), ответственного (ответственных) за обеспечение функционирования информационных систем и их компонентов (далее – подразделение (подразделения), ответственное (ответственные) за обеспечение функционирования информационных систем), по исполнению политики информационных систем и требований настоящей главы;

должностное лицо (лицо, его замещающее), ответственное за обеспечение функционирования информационных систем кредитной организации (головной кредитной организации банковской группы) и координацию деятельности подразделения (подразделений), ответственного (ответственных) за обеспечение функционирования информационных систем (далее – должностное лицо, ответственное за информационные системы);

перечень информационных систем, обеспечивающих функционирование процессов;

требования к информационным системам, в том числе требования по обеспечению непрерывности и качества функционирования информационных систем;

порядок информационного взаимодействия в рамках реализации политики информационных систем;

порядок и периодичность формирования отчетов должностного лица, ответственного за информационные системы, и подразделения (подразделений), ответственного (ответственных) за обеспечение функционирования информационных систем, направляемых на рассмотрение коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы).

Политика информационных систем утверждается коллегиальным исполнительным органом кредитной организации (головной кредитной организации банковской группы).

Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) несет ответственность за соблюдение требований политики информационных систем.

8.4. Должностное лицо, ответственное за информационные системы, проводит не реже одного раза в год анализ необходимости пересмотра требований политики информационных систем в зависимости от осуществляемых операций и (или) действующих процессов, изменяющихся внешних факторов и стратегических планов развития кредитной организации (головной кредитной организации банковской группы), результатов процедур управления операционным риском, результатов оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, и направляет результаты анализа на рассмотрение коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы) для принятия решения о необходимости внесения изменений в политику информационных систем и внутренние документы.

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок и правила проведения анализа и пересмотра политики информационных систем.

8.5. Кредитная организация (головная кредитная организация банковской группы) определяет в политике информационных систем перечень информационных систем, обеспечивающих функционирование процессов, в соответствии с подпунктом 4.1.1 пункта 4.1 настоящего Положения, в том числе требующих обеспечение информационного взаимодействия, обработку и хранение информации с помощью информационных систем.

8.6. Кредитная организация (головная кредитная организация банковской группы) обеспечивает проведение подразделениями кредитной

организации (головной кредитной организации банковской группы) мероприятий, направленных на выявление, оценку, разработку форм (способов) контроля, и мероприятий, направленных на повышение качества системы управления риском информационных систем и снижение уровня риска информационных систем и сопряженных с ним рисков информационной безопасности, влияющих на информационные системы (в том числе рисков уничтожения (искажения, безвозвратного удаления) носителей и (или) хранилищ информации и данных, хранящихся в информационных системах).

8.7. Кредитная организация (головная кредитная организация банковской группы) в целях управления риском информационных систем разрабатывает во внутренних документах и соблюдает требования к информационным системам с учетом их влияния на обеспечение бесперебойной работы процессов кредитной организации (головной кредитной организации банковской группы).

8.7.1. Требования к структуре информационных систем, включая требования к:

составу основных функций, компонентов, подсистем информационных систем и их иерархической структуры в соответствии с заданными кредитной организацией (головной кредитной организацией банковской группы) функциональными требованиями и техническими заданиями;

средствам и способам обмена информации между подсистемами информационных систем в случае распределенной архитектуры, в том числе с элементами, размещенными у внешних поставщиков услуг и информации (провайдеров, операторов связи или других контрагентов);

архитектуре взаимодействия со смежными информационными системами, в том числе третьих лиц и провайдеров.

8.7.2. Требования к стандартизации и унификации, используемые при создании, модернизации и эксплуатации информационных систем, включая требования к:

перечню используемых кредитной организацией (головной кредитной организацией банковской группы) программных и технических средств;

перечню программно-аппаратных решений, требующих лицензирования и сертификации;

правилам разработки (как собственными силами кредитной организации (головной кредитной организации банковской группы), так и силами привлеченных подрядчиков), приемки, тестирования, сопровождения информационных систем и ведения рабочей документации, включая порядок хранения и изменения исходного кода (в том числе раздельное хранение, исключающее доступ разработчиков);

классификации информационных систем с учетом критичности и влияния информационных систем на процессы, а также влияния сбоев в работе информационных систем на процессы кредитной организации (головной кредитной организации банковской группы);

квалификации работников, задействованных при разработке и эксплуатации информационных систем;

закупке услуг и информации в случае необходимости привлечения внешних поставщиков услуг и информации, в том числе порядку выбора поставщиков, определения их ответственности и правил их взаимодействия;

критериям и порядку определения технической и экономической целесообразности передачи на аутсорсинг элементов информационных систем с учетом рисков утраты доступа к этим элементам информационных систем и утраты данных, а также порядку контроля кредитной организации (головной кредитной организации банковской группы) за элементами информационных систем, переданными на аутсорсинг.

8.7.3. Требования к надежности функционирования информационных систем, включая требования к:

порядку выявления и устранения сбоев информационных систем, включающему перечень возможных отказов и (или) сбоев информационных систем или их элементов, их классификацию и примерные варианты решения,

а также к информационному, техническому и программному обеспечению информационных систем;

режимам функционирования информационных систем (например, период доступности системы в течение суток, максимальное допустимое время простоя в год, допустимые интервалы в случае установки обновления);

аутсорсингу обслуживания и функционирования информационных систем, включая обязательные мероприятия по обеспечению сохранности элементов информационных систем, переданных на аутсорсинг, доступа к ним и контроля кредитной организации (головной кредитной организации банковской группы) за ними, в том числе персональную ответственность должностных лиц за сохранность информационных систем и данных, переданных на аутсорсинг;

перечню показателей надежности функционирования информационных систем и их пороговым значениям;

инструментам, методам контроля и способам оценки надежности функционирования информационных систем кредитной организации (головной кредитной организации банковской группы);

проведению мероприятий по повышению качества функционирования информационных систем;

периоду коммерческого использования с сохранением требуемых функций информационных систем (жизненному циклу информационных систем);

другие требования, отражающие особенности обеспечения функционирования процессов и структуры информационных систем кредитной организации (головной кредитной организации банковской группы).

8.7.4. Требования к обеспечению качества данных в информационных системах в разрезе характеристик качества данных в рамках обеспечения функционирования процессов, включая требования к:

точности и достоверности 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;

полноте данных в части достаточности объема данных (количеству хранящихся в информационных системах записей), глубине данных (периоду данных, используемому для проведения операций и оценки эффективности процессов, применяемых методик и моделей процессов) и широте данных (охвату данными всех разрезов, свойств и характеристик объектов), требуемым в рамках обеспечения функционирования процессов;

свойствам данных в любой момент времени адекватно отражать состояние объектов предметной области (актуальность данных);

взаимной непротиворечивости данных, хранящихся в информационных системах кредитной организации (головной кредитной организации банковской группы), других источниках и носителях информации, унификации данных при их перемещении в информационных системах и процессах, целостности соответствующих идентификационных ссылок и связей в структурах баз данных (согласованность данных);

возможности использования данных при функционировании процессов (доступность данных);

возможности осуществления контроля качества и происхождения данных, в том числе посредством отражения в информационных системах источников данных, истории создания, изменения, преобразования, удаления, хранения и передачи данных (контролируемость данных);

возможности сохранять установленный уровень функциональности и качества данных после их утраты, повреждения или изменения в результате сбоев или других нарушений функционирования информационных систем (восстанавливаемость данных);

другим характеристикам качества данных, определяемым кредитной организацией (головной кредитной организацией банковской группы) во внутренних документах.

Кредитная организация (головная кредитная организация банковской группы) с учетом осуществляемых операций и (или) действующих процессов, уровня и сочетания принимаемых рисков, текущих и стратегических планов развития и доступных возможностей определяет во внутренних документах дополнительные характеристики качества данных в информационных системах, включающие разработку методики обеспечения качества данных и порядка обеспечения качества данных.

8.7.5. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах методику обеспечения качества данных в информационных системах, обеспечивающих критически важные процессы, включающую следующие элементы:

классификатор возможных источников и причин образования в информационных системах данных, не соответствующих требованиям к качеству данных в информационных системах;

показатели (индикаторы) качества данных для оценки характеристик качества данных, разрабатываемые кредитной организацией (головной кредитной организацией банковской группы) для различных информационных систем;

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 во внутренних документах другие элементы методики обеспечения качества данных в информационных системах.

Кредитная организация (головная кредитная организация банковской группы) применяет элементы методики обеспечения качества данных с учетом

особенностей конкретных данных, в том числе методов и процедур их фиксирования, хранения и преобразования, а также их типов и форматов.

8.7.6. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок обеспечения качества данных в информационных системах, 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, критериев оценки качества данных;

процедуры, правила и периодичность контроля качества данных и формирования отчетов о качестве данных, о проведении мероприятий контроля качества данных;

процедуры исправления выявленных ошибок в данных и документирования внесенных в них изменений;

порядок взаимодействия органов управления, подразделений и должностных лиц кредитной организации (головной кредитной организации банковской группы) по вопросам обеспечения качества данных, устанавливающий их полномочия, ответственность, подотчетность и обеспеченность ресурсами, в том числе определяющий в кредитной организации (головной кредитной организации банковской группы) должностное лицо (должностные лица), несущее (несущие) персональную ответственность за обеспечение качества данных в информационных системах;

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

Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах другие элементы порядка обеспечения качества данных в информационных системах.

8.7.7. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах дополнительные требования к информационным системам и их функционированию с учетом осуществляемых операций и (или) действующих процессов, уровня и сочетания принимаемых рисков, текущих и стратегических планов развития и доступных возможностей.

8.7.8. Подразделение (подразделения), ответственное (ответственные) за обеспечение функционирования информационных систем, не реже одного раза в год проводит (проводят) анализ необходимости пересмотра требований к информационным системам с учетом текущих и стратегических планов развития, их влияния на процессы, оценки уровня операционного риска, отраженной в отчетах по операционному риску, и мероприятий, направленных на повышение качества системы операционным риском и уменьшение негативного влияния операционного риска, а также с учетом отчетов службы информационной безопасности и подразделения, ответственного за обеспечение информационной безопасности, и направляет результаты анализа коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы) для принятия решения о пересмотре требований к информационным системам.

8.8. Кредитная организация (головная кредитная организация банковской группы) устанавливает во внутренних документах и соблюдает следующие требования по обеспечению непрерывности и качества функционирования информационных систем.

8.8.1. Разработка, реализация и контроль выполнения требований к информационным системам, обеспечивающим функционирование системы информационной безопасности в соответствии с пунктом 7.7 настоящего Положения.

8.8.2. Обеспечение условий эксплуатации технических средств элементов информационных систем, 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 процессов на резервные технические средства, размещенные не в тех зданиях, в которых размещены действующие технические средства, обеспечивающие функционирование информационных систем в текущем рабочем режиме. Кредитная организация (головная кредитная организация банковской группы) обеспечивает надежность функционирования резервных технических средств, в том числе соблюдение требования подпункта 8.8.2 настоящего пункта, режима охраны и доступа.

8.8.4. Использование программного обеспечения, принятого в эксплуатацию с соблюдением требований подпункта 8.7.2 пункта 8.7 настоящего Положения и технических условий эксплуатации, описанных в эксплуатационной документации программного обеспечения кредитной организации (головной кредитной организации банковской группы).

8.8.5. Наличие во внутренних документах кредитной организации (головной кредитной организации банковской группы) положения и стратегии по обеспечению непрерывности и восстановления функционирования информационных систем. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах орган кредитной организации (головной кредитной организации банковской группы), который утверждает стратегию и положение по обеспечению непрерывности и восстановления функционирования информационных систем, с установлением обязательств соблюдения требований внутренних документов всеми подразделениями кредитной организации (головной кредитной организация банковской группы).

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

8.8.7. Ежегодное тестирование уязвимостей информационных систем и (или) их компонентов и других источников риска информационных систем, а также разработка комплекса мероприятий, направленных на устранение выявленных уязвимостей информационных систем и (или) других источников риска информационных систем.

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

соблюдения политики информационных систем;

мероприятий, направленных на повышение качества системы управления риском информационных систем и уменьшение негативного влияния риска информационных систем;

требований к информационным системам в целях управления риском информационных систем;

требований по обеспечению непрерывности и качества функционирования информационных систем.

Уполномоченное подразделение направляет отчеты по результатам оценки соблюдения требований, установленных настоящей главой, совету директоров (наблюдательному совету) и коллегиальному исполнительному органу кредитной организации (головной кредитной организации банковской группы), подразделению (подразделениям), ответственному (ответственным)

за обеспечение функционирования информационных систем, и службе управления рисками.

8.8.9. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) определяет подразделение (подразделения), ответственное (ответственные) за обеспечение непрерывности функционирования информационных систем, 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 подразделения, в том числе 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 информационных систем в кредитной организации (головной кредитной организации банковской группы), включая его полномочия и требования к его квалификации.

8.8.11. Должностное лицо (лицо, его замещающее), ответственное за обеспечение непрерывности функционирования информационных систем в кредитной организации (головной кредитной организации банковской группы), регулярно (не реже одного раза в год) проводит самооценку рисков информационных систем в разрезе процессов с учетом требований настоящей главы и направляет отчеты по результатам самооценки в подразделение, ответственное за организацию управления операционным риском, и (или) другому органу, установленному кредитной организацией (головной кредитной организацией банковской группы) во внутренних документах.

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

8.8.13. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах дополнительные требования к обеспечению непрерывности и качества функционирования информационных систем с учетом осуществляемых операций и (или) действующих процессов, принимаемых рисков, текущих и стратегических планов развития и доступных возможностей.

Глава 9. Соблюдение требований настоящего Положения кредитными организациями (головной кредитной организацией банковской группы)

9.1. Банк, размер активов которого составляет 500 миллиардов рублей и более на начало текущего отчетного года в соответствии со значением статьи «Всего активов», определяемым в соответствии с Разработочной таблицей для составления бухгалтерского баланса (публикуемой формы) пункта 3 Порядка составления и представления отчетности по форме 0409806 «Бухгалтерский баланс (публикуемая форма)», установленного приложением 1 к Указанию Банка России № 4927-У (далее – банк, размер активов которого составляет 500 миллиардов рублей и более):

9.1.1. обязан соблюдать:

требования глав 1, 3–8 настоящего Положения и приложений 1, 2, 4, 5 к настоящему Положению;

требования абзацев первого – четвертого подпункта 2.1.1, подпунктов 2.1.2–2.1.4, абзацев первого – второго, четвертого – тринадцатого, шестнадцатого –

семнадцатого подпункта 2.1.5, подпунктов 2.1.6–2.1.7 пункта 2.1, пунктов 2.2–2.5 главы 2 настоящего Положения;

9.1.2. вправе самостоятельно определить во внутренних документах другие способы управления операционным риском из указанных в пункте 2.1 настоящего Положения в дополнение к способам управления операционным риском, указанным в абзаце третьем подпункта 9.1.1 настоящего пункта.

9.2. Банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей на начало текущего отчетного года в соответствии со значением статьи «Всего активов», определяемым в соответствии с Разработочной таблицей для составления Бухгалтерского баланса (публикуемой формы) пункта 3 Порядка составления и представления отчетности по форме 0409806 «Бухгалтерский баланс (публикуемая форма)», установленного приложением 1 к Указанию Банка России № 4927-У (далее – банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей):

9.2.1. обязан соблюдать:

требования глав 1, 3, 5–8 настоящего Положения и приложений 1, 2, 4, 5 к настоящему Положению,

требования абзацев первого – третьего подпункта 2.1.1, подпункта 2.1.2 (банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, с учетом порога регистрации фиксирует в базе событий события операционного риска с прямыми и (или) косвенными потерями, а также потерями, указанными в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения), подпункта 2.1.3, абзацев первого – третьего, пятого подпункта 2.1.4, абзацев первого, второго, четвертого – тринадцатого подпункта 2.1.5, абзацев шестнадцатого и семнадцатого подпункта 2.1.5 (в случае, если банк с универсальной лицензией, размер активов которого составляет менее 500 миллиардов рублей, использует методы оценки величины риска и общей потребности в капитале, отличные от

установленных Банком России в соответствии с пунктом 5.1 Указания Банка России № 3624-У), подпунктов 2.1.6 и 2.1.7 пункта 2.1, пунктов 2.2–2.5 главы 2 настоящего Положения;

требования пунктов 4.1–4.2, 4.4 – 4.6 главы 4 настоящего Положения;

9.2.2. вправе самостоятельно определить во внутренних документах другие способы управления операционным риском из указанных в пункте 2.1 настоящего Положения, в дополнение к способам управления операционным риском, указанным в третьем абзаце подпункта 9.2.1 настоящего пункта.

9.3. Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является банком с базовой лицензией (далее – банк с базовой лицензией):

9.3.1. обязана соблюдать:

требования глав 1, 3, 5 – 7 настоящего Положения и приложений 2, 4, 5 к настоящему Положению;

требования абзацев первого – второго подпункта 2.1.1, абзацев первого, третьего – четырнадцатого подпункта 2.1.2 (при этом банк с базовой лицензией с учетом порога регистрации фиксирует в базе событий события операционного риска с прямыми потерями, а также потерями, указанными в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения), подпункта 2.1.3, абзацев первого – третьего подпункта 2.1.4, абзацев первого – двенадцатого подпункта 2.1.6 (в части соблюдения требований абзацев первого – двенадцатого подпункта 2.1.6 пункта 2.1 настоящего Положения банк с базовой лицензией обеспечивает выбор и применение способа реагирования, в том числе принятие мер, направленных на уменьшение негативного влияния операционного риска, только в части реализовавшихся событий операционного риска с прямыми потерями) пункта 2.1, пунктов 2.2–2.5 главы 2 настоящего Положения;

требования пунктов 4.1, 4.2, 4.4 – 4.6 главы 4 настоящего Положения;

требования пунктов 8.1–8.5, пункта 8.6 (в части выявления риска информационной безопасности), абзацев шестого и седьмого подпункта 8.7.2, абзацев первого, третьего и четвертого подпункта 8.7.3, абзацев первого – восьмого подпункта 8.7.4 пункта 8.7, подпунктов 8.8.1–8.8.5, подпунктов 8.8.8–8.8.10, подпунктов 8.8.12–8.8.13 пункта 8.8 главы 8 настоящего Положения;

требования абзацев второго – восьмого, одиннадцатого подпункта 1.1.1, подпунктов 1.1.2, 1.1.3 и 1.2 пункта 1 приложения 1 к настоящему Положению;

9.3.2. вправе самостоятельно определить во внутренних документах другие способы управления операционным риском из указанных в пункте 2.1 настоящего Положения в дополнение к способам управления операционным риском, указанным в абзаце третьем подпункта 9.3.1 настоящего пункта.

9.4. Кредитная организация (головная кредитная организация банковской группы), которая на начало текущего отчетного года является небанковской кредитной организацией (далее – НКО), обязана соблюдать:

требования глав 1, 3, 6 настоящего Положения и приложений 4 и 5 к настоящему Положению;

требования абзацев первого и второго подпункта 2.1.1, абзацев первого, третьего – четырнадцатого подпункта 2.1.2 (при этом НКО с учетом порога регистрации фиксирует в базе событий события операционного риска с прямыми потерями, потерями, указанными в абзаце втором подпункта 3.13.3 пункта 3.13 настоящего Положения), подпункта 2.1.3, абзацев первого и второго подпункта 2.1.4, абзацев первого – двенадцатого подпункта 2.1.6 (НКО обеспечивает выбор и применение способа реагирования, в том числе принятие мер, направленных на уменьшение негативного влияния операционного риска, только в части реализовавшихся событий операционного риска с прямыми потерями) пункта 2.1, пунктов 2.2–2.5 главы 2 настоящего Положения;

требования подпункта 4.1.4 пункта 4.1, пункта 4.4 главы 4 настоящего Положения;

требования пунктов 7.1–7.7, абзацев первого – третьего, пятого – девятого пункта 7.8, подпункта 7.9.1, абзацев первого – шестого, восьмого – десятого подпункта 7.9.2 пункта 7.9, пункты 7.10 и 7.11 главы 7 настоящего Положения.

9.4.1. Порядок осуществления НКО, имеющей право на осуществление переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций (далее – платежная НКО), контроля за уровнем операционного риска при привлечении банковского платежного агента в соответствии со статьей 14 Федерального закона № 161-ФЗ (Собрание законодательства Российской Федерации, 2011, № 27, ст. 3872; 2019, № 27, ст. 3538) должен включать в себя:

порядок сбора и анализа платежной НКО информации о банковском платежном агенте;

порядок распределения полномочий между подразделениями и служащими платежной НКО при привлечении банковского платежного агента;

порядок выявления, оценки, мониторинга платежной НКО операционных рисков, связанных с привлечением банковского платежного агента, а также осуществления платежной НКО мер по достижению и (или) поддержанию их приемлемого уровня;

порядок осуществления платежной НКО контроля за деятельностью банковского платежного агента;

порядок обеспечения платежной НКО переводов денежных средств без открытия банковских счетов и связанных с ними иных банковских операций в случае несоблюдения банковским платежным агентом условий его привлечения (включая обеспечение возможности использования услуг

другого банковского платежного агента или переход на самообслуживание);

порядок составления и периодичность представления в органы управления, определенные внутренними документами платежной НКО, отчета о результатах контроля за уровнем операционного риска при привлечении банковского платежного агента.

9.4.2. НКО вправе самостоятельно определить во внутренних документах другие способы управления операционным риском из указанных в пункте 2.1 настоящего Положения в дополнение к способам управления операционным риском, указанным в абзаце третьем настоящего пункта.

Глава 10. **Заключительные положения**

10.1. Настоящее Положение подлежит официальному опубликованию и в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от 20 марта 2020 года № 6) вступает в силу с 1 октября 2020 года.

10.2. Система управления операционным риском подлежит приведению в соответствие с требованиями настоящего Положения кредитными организациями (головными кредитными организациями банковской группы), в срок до 1 января 2022 года.

10.3. Кредитные организации (головные кредитные организации банковской группы) в случае приведения системы управления операционным риском в соответствие с требованиями настоящего Положения ранее 1 января 2022 года, вправе проинформировать об этом Банк России в целях организации Банком России оценки соответствия системы управления операционным риском требованиям настоящего Положения.

10.4. С 1 января 2022 года признать утратившим силу Указание Банка России от 25 июня 2012 года № 2840-У «О требованиях к управлению операционным риском небанковскими кредитными организациями, имеющими право на осуществление переводов денежных средств без

открытия банковских счетов и связанных с ними иных банковских операций», зарегистрированное Министерством юстиции Российской Федерации 26 июня 2012 года № 24690.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение 1
к Положению Банка России
от 8 апреля 2020 года № 716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Контрольные показатели уровня операционного риска

1. Кредитная организация (головная кредитная организация банковской группы) определяет во внутренних документах порядок установления и контроля соблюдения следующих контрольных показателей уровня операционного риска в соответствии с главами 5 и 9 настоящего Положения.

1.1. Базовый набор показателей системы управления операционным риском включает следующие показатели.

1.1.1. Количественные контрольные показатели:

общая сумма валовых прямых потерь, понесенных кредитной организацией от реализации событий операционного риска за вычетом потерь от реализации событий риска информационной безопасности за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;

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

отношение общей суммы чистых (фактических) прямых потерь (включая чистые (фактические) прямые потери от реализации событий риска информационной безопасности), понесенных кредитной организацией за год, к показателю объема операционного риска в виде показателя Д, рассчитанного в соответствии с пунктом 3 Положения Банка России № 652-П на последнюю отчетную дату (далее – показатель объема операционного риска);

отношение общей суммы валовых прямых потерь от реализации событий операционного риска за вычетом потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией за год, к показателю объема операционного риска;

отношение суммы чистых (фактических) прямых потерь от реализации событий операционного риска, рассчитанных в соответствии с пунктом 6.18 настоящего Положения, понесенных кредитной организацией за год, за вычетом потерь от реализации событий риска информационной безопасности к показателю объема операционного риска;

доля выявленных (по количеству) в ходе оценки эффективности функционирования системы управления операционным риском, проведенной уполномоченным подразделением, внешним экспертом или Банком России, событий операционного риска с валовыми прямыми потерями, превышающими порог регистрации (за исключением потерь от реализации событий кредитного риска, связанного с реализацией операционного риска), определяемый 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 валовыми прямыми потерями (за исключением потерь от реализации кредитного риска), превышающими порог регистрации (за исключением потерь от кредитного риска), за годовой период, к которому относится проверяемый период (контрольное значение должно быть не больше 5 процентов, сигнальное значение – не больше 3 процентов);

отношение сумм валовых прямых потерь от реализации 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 реализации событий кредитного риска, связанных с реализацией операционного риска), определяемый в соответствии с пунктом 6.5

настоящего Положения, которые кредитная организация не отразила в базе событий, к общей сумме валовых прямых потерь от реализации всех событий операционного риска, зарегистрированных в базе событий с прямыми потерями (за исключением потерь от реализации событий кредитного риска, связанных с реализацией операционного риска), превышающими порог регистрации, за годовой период, к которому относится проверяемый период (контрольное значение должно быть не больше 5 процентов, сигнальное значение – не больше 3 процентов);

общая сумма валовых прямых и косвенных потерь от реализации событий операционного риска, определяемых расчетным образом, за вычетом потерь от реализации событий риска информационной безопасности, за определенный период (первый квартал, полугодие, девять месяцев, год) с начала календарного года;

отношение суммы чистых (фактических) прямых и косвенных потерь от реализации событий операционного риска, определяемых расчетным образом, за вычетом потерь от реализации событий риска информационной безопасности к общему капиталу (собственным средствам) кредитной организации на последнюю отчетную дату года;

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

1.1.2. Качественные контрольные показатели, к которым 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;

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

1.1.3. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) 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 процессов, подразделениям, видам операционного риска (риск информационной безопасности, риск информационных систем, операционный риск в целом) в соответствии с абзацами вторым – восьмым, одиннадцатым подпункта 1.1.1 настоящего пункта.

1.2. Базовый набор контрольных показателей уровня риска информационной безопасности включает следующие показатели.

1.2.1. Количественные контрольные показатели риска информационной безопасности:

общая сумма валовых прямых потерь от реализации событий риска информационной безопасности за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;

общая сумма валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах, в соответствии с подпунктом 1.1 пункта 1 приложения 5 к настоящему Положению за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;

отношение общей суммы чистых (фактических) прямых потерь от реализации событий риска информационной безопасности, понесенных кредитной организацией за отчетный период (первый квартал, полугодие, девять месяцев, год), к базовому капиталу кредитной организации на последнюю отчетную дату года;

отношение суммы валовых прямых потерь, понесенных кредитной организацией при выполнении кредитной организацией функций участника

платежной системы Банка России, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме операций по переводу денежных средств через платежную систему Банка России за этот же период (контрольное значение должно быть не более 0,05 процента, сигнальное значение – не более 0,005 процента);

отношение суммы валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах, в соответствии с подпунктом 1.1 пункта 1 приложения 5 к настоящему Положению за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов денежных средств и платежей в платежных системах за этот же период (контрольное значение должно быть не более 0,05 процента, сигнальное значение – не более 0,005 процента);

отношение суммы денежных средств, по которой получены уведомления клиентов о несанкционированном переводе (списании) денежных средств, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов за этот же период (контрольное значение должно быть не более 0,05 процентов, сигнальное значение – не более 0,005 процента);

доля реализованных (по количеству), то есть не предотвращенных системой информационной безопасности кредитной организации, событий риска информационной безопасности с ненулевой величиной валовых прямых потерь по отношению ко всем событиям риска информационной безопасности, зарегистрированным в базе событий, с ненулевой величиной валовых прямых потерь в течение отчетного периода (первого квартала, полугодия, девяти месяцев, года), о которых кредитная организация сообщила в своих отчетах в Банк России, направляемых в соответствии пунктом 8 Положения Банка России № 683-П;

доля выявленных (по количеству) в ходе оценки эффективности функционирования системы управления операционным риском, проведенной

уполномоченным подразделением, внешним экспертом или Банком России, событий риска информационной безопасности с ненулевой величиной валовых прямых потерь, о которых кредитная организация не сообщила в своих отчетах в Банк России, направляемых в соответствии пунктом 8 Положения Банка России № 683-П, по отношению ко всем зарегистрированным событиям риска информационной безопасности с ненулевой величиной валовых прямых потерь, о которых кредитная организация сообщила в своих отчетах в Банк России, направляемых в соответствии с пунктом 8 Положения Банка России № 683-П;

общая сумма валовых прямых и косвенных потерь от реализации событий риска информационной безопасности за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска (в случае, если кредитная организация применяет подход количественной оценки потерь от реализации операционного риска на основе статистики базы событий (с использованием статистики за период не менее пяти лет) с использованием методов, применяемых в международной практике (далее – продвинутый подход);

отношение суммы чистых (фактических) прямых и косвенных потерь от событий риска информационной безопасности к собственным средствам (капиталу) кредитной организации на последнюю отчетную дату года (в случае, если кредитная организация применяет продвинутый подход к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска);

отношение суммы валовых прямых и косвенных потерь, понесенных кредитной организацией при выполнении кредитной организацией функций оператора других платежных систем или оператора услуг платежной инфраструктуры, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме операций по переводу денежных средств через другие платежные системы или

платежную инфраструктуру за этот же период (в случае, если кредитная организация применяет продвинутый подход к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска);

общая сумма валовых прямых и косвенных потерь кредитной организации в результате использования электронных средств платежа клиентов кредитных организаций без их согласия за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года (в случае, если кредитная организация применяет продвинутый подход к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска);

общая сумма валовых прямых и косвенных потерь кредитной организации в результате переводов и снятия денежных средств, связанных с несанкционированным доступом к объектам информационной инфраструктуры кредитной организации, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года (в случае, если кредитная организация применяет продвинутый подход к расчету объема капитала, выделяемого на покрытие потерь от реализации операционного риска).

1.2.2. Качественные контрольные показатели риска информационной безопасности, к которым относятся качественные оценки по четырехуровневой системе («хорошо», «удовлетворительно», «сомнительно», «неудовлетворительно») по следующим направлениям:

оценка эффективности функционирования системы управления риском информационной безопасности, проведенная уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета) кредитной организации;

для кредитных организаций – участников платежной системы Банка России – оценка соблюдения кредитной организацией требований Положения Банка России № 382-П, Положения Банка России № 683-П, Положения Банка

России от 9 января 2019 года № 672-П «О требованиях к защите информации в платежной системе Банка России», зарегистрированного Министерством юстиции Российской Федерации 21 марта 2019 года № 54109;

для кредитных организаций – независимая оценка соответствия уровня защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы) в соответствии с требованиями пункта 9 Положения Банка России № 683-П.

2. Дочерние кредитные организации, осуществляющие свою деятельность в иностранной юрисдикции, в случае противоречия национального законодательства требованиям настоящего Положения приводят в соответствие с требованиями национального законодательства показатели, указанные в настоящем приложении.

Приложение 2
к Положению Банка России
от 8 апреля 2020 года № 716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Подходы к расчету объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации операционного риска

1. Кредитная организация (головная кредитная организация банковской группы) в целях соблюдения требований абзаца третьего подпункта 2.1.4 пункта 2.1 настоящего Положения выбирает один из следующих подходов к расчету объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска:

регуляторный подход на базе расчета размера 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 (далее – регуляторный подход);

продвинутый подход.

2. В случае если объем капитала, выделяемого на покрытие потерь от реализации событий операционного риска, 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 (головной кредитной организации банковской группы) в составе материалов, направляемых в совет директоров (наблюдательный совет) для утверждения стратегии управления рисками и капиталом, представляет заключение, содержащее обоснование того, что уровень операционного риска в кредитной организации (головной кредитной организации банковской группы)

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 капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, по формуле:

$$К_{необ\_Ki,ОР} = К_{мин\_Ki,ОР} + \Delta_{Ki,ИБ} + \Delta_{Ki,ОР},$$

где:

$К_{необ\_Ki,ОР}$ – объем капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, включаемый в состав совокупного объема необходимого капитала, соответствующего показателю $К_i$, определенному в соответствии с подпунктом 2.1.1 пункта 2.1 Инструкции Банка России от 29 ноября 2019 года № 199-И «Об обязательных нормативах и надбавках к нормативам достаточности капитала банков с универсальной лицензией», зарегистрированной Министерством юстиции Российский Федерации 27 декабря 2019 года № 57008 (далее – Инструкция Банка России № 199-И);

$К_{мин\_Ki,ОР}$ – минимальный регуляторный капитал на покрытие потерь от реализации событий операционного риска, включаемый в состав совокупного объема необходимого капитала, соответствующего показателю $К_i$, и выделяемый на покрытие потерь от реализации событий операционного риска, необходимый для соблюдения минимально допустимого числового значения норматива достаточности капитала $Н1.i$, установленного для кредитной организации в соответствии с подпунктом 2.1.1 пункта 2.1 Инструкции Банка России № 199-И и для головной кредитной организации банковской группы в соответствии с пунктом 2.1 Положения Банка России № 509-П, определяемый по формуле:

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

где:

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

$Н1.i_{мин}$ – минимально допустимое числовое значение норматива достаточности капитала Н1.i, определенное в пункте 2.2 Инструкции Банка России № 199-И;

$\Delta_{К i,ИБ}$ – компонент объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, соответствующего: $К_1$ – базовому капиталу банка, $К_2$ – основному капиталу банка, $К_0$ – величине собственных средств (капитала) банка, определенных в соответствии с методикой, установленной Положением Банка России № 646-П, соответственно на покрытие прямых потерь (для $\Delta_{К1,ИБ}$ и $\Delta_{К2,ИБ}$), совокупных (прямых и косвенных) потерь (для $\Delta_{К0,ИБ}$) от реализации событий риска информационной безопасности, которые определяются кредитной организацией (головной кредитной организацией банковской группы) на базе сценарного анализа в части возможного превышения фактической величины прямых (совокупных) потерь над контрольным значением контрольного показателя – лимита прямых (совокупных) годовых потерь от реализации событий риска информационной безопасности, установленного в соответствии подпунктом 1.2.1 пункта 1 приложения 1 к настоящему Положению;

$\Delta_{Кi,ОР}$ – компонент объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, соответствующего: $К_1$ – базовому капиталу банка, $К_2$ – основному капиталу банка, $К_0$ – величине собственных средств (капитала) банка, определенных в соответствии с методикой, предусмотренной Положением Банка России

№ 646-П, соответственно на покрытие прямых потерь (для $\Delta_{К1,ОР}$ и $\Delta_{К2,ОР}$), совокупных (прямых и косвенных) потерь для ($\Delta_{К0,ОР}$) от реализации операционного риска, за вычетом потерь от реализации событий риска информационной безопасности, которые определяются кредитной организацией (головной кредитной организацией банковской группы) на базе сценарного анализа 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 информационной безопасности, установленного в соответствии с подпунктом 1.1.1 пункта 1 приложения 1 к настоящему Положению.

4. В случае если кредитная организация (головная кредитная организация банковской группы) применяет регуляторный подход к оценке объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, и фактическая совокупная величина прямых годовых потерь от реализации событий операционного риска и событий риска информационной безопасности за каждый год не превышала минимальный регуляторный капитал, рассчитанный для данного года, на протяжении последних десяти лет, кредитная организация (головная кредитная организация банковской группы) приравнивает к нулю компонент объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий риска информационной безопасности и (или) событий операционного риска, в соответствии с заключением службы управления рисками об отсутствии других факторов возможных потерь (например, об отсутствии изменений внутренних и внешних факторов операционной среды кредитной организации (головной кредитной организации банковской группы) с приложением результатов сценарного анализа и стресс-тестирования.

4.1. В случае если у кредитной организации (головной кредитной организации банковской группы) отсутствуют данные о потерях от реализации событий операционного риска и событий риска информационной безопасности за десять лет, кредитная организация (головная кредитная организация банковской группы) использует в целях расчета объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, накопленные данные за имеющейся период, но не менее чем за три года (с последующим учетом накопленных данных о потерях до достижения периода десяти лет), для сравнения с минимальным регуляторным капиталом за каждый год в течение периода десяти лет.

При этом кредитная организация (головная кредитная организация банковской группы) ежегодно при формировании объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, готовит заключение о достаточности имеющихся накопленных данных о потерях от реализации событий операционного риска и (или) событий риска информационной безопасности для установления нулевых значений компонентов объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска и (или) событий риска информационной безопасности.

4.2. Коллегиальный исполнительный орган кредитной организации (головной кредитной организации банковской группы) рассматривает заключение об отсутствии других факторов возможных потерь от реализации операционных рисков и утверждает его в рамках внутренних процедур планирования объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска.

4.3. В случае если у кредитной организации (головной кредитной

организации банковской группы) отсутствуют данные о потерях от реализации событий операционного риска и (или) событий риска информационной безопасности за три года или накопленные данные не соответствуют требованиям главы 6 настоящего Положения, за исключением абзаца тридцать первого и сорок четвертого пункта 6.6 настоящего Положения, кредитная организация (головная кредитная организация банковской группы) не устанавливает нулевые значения компонентов $\Delta_{Ki,ИБ}$ и $\Delta_{Ki,ОР}$ и при определении объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, должна определять значение данных компонентов с учетом сценарного анализа.

4.4. Подразделение, ответственное за организацию управления операционным риском, подготавливает заключение об отсутствии других факторов возможных потерь от реализации 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, определяет объем капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, в составе капитала $К_i$ в соответствии с методикой количественной оценки прямых потерь (для объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, в составе базового и основного капиталов) и совокупных потерь (для объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, в составе собственных средств) от реализации событий операционного риска (методика потерь), с заданной во внутренних документах доверительной вероятностью как сумму двух компонентов:

объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий риска информационной безопасности;

объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации операционного риска, за вычетом потерь от реализации риска информационной безопасности.

При этом для оценки объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, в дополнение к потерям от реализации внутренних событий операционного риска кредитная организация (головная кредитная организация банковской группы) должна использовать внешнюю информацию о потерях других кредитных организаций с применением методов сценарного анализа в соответствии с пунктом 4.4 приложения 1 к Указанию Банка России № 3624-У.

6. В случае если фактическая величина потерь от реализации событий операционного риска и (или) событий риска информационной безопасности по итогам года превысила выделенную на этот год величину объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, данное превышение добавляется кредитной организацией (головной кредитной организацией банковской группы) в течение последующего года к оценке компонентов объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, рассчитанной по потерям из базы событий.

7. Кредитная организация (головная кредитная организация банковской группы), учитывающая потери от реализации операционного риска и (или) риска информационной безопасности в запланированных расходах кредитной организации (головной кредитной организации банковской группы) того года,

в котором были отражены потери, при определении сигнального значения прямых или совокупных потерь уменьшает компоненты объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, на величину, не превышающую величину запланированных расходов от реализации операционного риска и (или) риска информационной безопасности.

8. Кредитная организация (головная кредитная организация банковской группы), применяющая механизмы и процедуры управления отдельными видами операционного риска, в составе объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации событий операционного риска, выделяет дополнительные компоненты объема капитала, выделяемого кредитной организацией (головной кредитной организацией банковской группы) на покрытие потерь от реализации этих видов операционного риска.

Приложение 3
к Положению Банка России
от 8 апреля 2020 года № 716-П
«О требованиях к системе управления
операционным риском в кредитной
организации и банковской группе»

Рекомендуемый перечень возможных мер, направленных на уменьшение негативного влияния операционного риска

Кредитная организация (головная кредитная организация банковской группы) использует следующий рекомендуемый перечень возможных мер, направленных на уменьшение негативного влияния операционного риска, но не ограничивается им.

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

2. Применение стандартизированных форм внутренних документов кредитной организации.

3. Стандартизация операций (сделок).

4. Применение стандартизированных форм договоров с клиентами (контрагентами).

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

6. Подбор и аттестация персонала.

7. Разработка системы мотивации персонала.

8. Проведение тренингов и обучение персонала проведению сделок (операций).

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

10. Особый контроль за проведением крупных сделок (нестандартных сделок).

11. Контроль сделок (операций).

12. Формирование отчетов по сделкам (операциям).

13. Тестирование процессов, информационных и технологических систем кредитной организации.

14. Автоматизация процессов (операций), алгоритмизация сделок (операций).

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

16. Разграничение функций, ответственности и полномочий персонала при проведении сделок (операций).

17. Использование двойного контроля при проведении сделок (операций).

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

19. Установление и разделение прав доступа к информации и информационным системам.

20. Резервирование информации в информационных системах.

21. Установление и разделение прав доступа к использованию материальных и нематериальных активов.

22. Организация физической безопасности объектов и материальных активов кредитной организации.

23. Противодействие неправомерному использованию инсайдерской информации.

24. Контроль качества данных в процессах, информационных системах.

25. Процедуры ограничения на ввод данных в информационных системах.

26. Автоматический контроль вводимых данных в информационных системах.

27. Контроль сроков и рассылка уведомлений участникам процессов.

28. Автоматический контроль маршрута согласований сделок

(операций).

29. Мероприятия по повышению культуры управления рисками.

30. Система ключевых показателей деятельности, стимулирующая персонал эффективно управлять рисками.

31. Другие меры, направленные на уменьшение негативного влияния операционного риска.

Приложение 4
к Положению Банка России
от 8 апреля 2020 года № 716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Детализированная классификация типов событий операционного риска

Кредитная организация (головная кредитная организация банковской группы) в разрезе основной классификации типов событий операционного риска дополнительно классифицирует события операционного риска по следующим типам событий операционного риска:

1. Тип события операционного риска «преднамеренные действия персонала» включает:

1.1. неразрешенную деятельность, состоящую в преднамеренных действиях персонала, связанную с превышением работниками своих полномочий при проведении или одобрении сделки (осуществлении операций), закрепленных должностными инструкциями, внутренними документами или решениями единоличного или коллегиального исполнительного органа кредитной организации, без цели присвоения, уничтожения, хищения имущества, материальных и (или) нематериальных активов, но в целях получения нематериальной выгоды;

1.2. преднамеренные действия персонала в отношении имущества, материальных и (или) нематериальных активов кредитной организации и средств клиентов с целью их присвоения, уничтожения, хищения в целях получения материальной выгоды, в том числе с использованием коммерческого подкупа (коррупции).

2. Тип события операционного риска «преднамеренные действия третьих лиц» включает:

2.1. преднамеренные действия третьих лиц в отношении имущества, материальных и (или) нематериальных активов кредитной организации и

средств клиентов. К данному типу событий операционного риска 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 операционного риска относятся все виды кибератак, совершенных третьими лицами с применением объектов информационной инфраструктуры по отношению к информации и данным, содержащимся во внутренних информационных системах кредитной организации (реализация событий киберриска).

3. Тип события операционного риска «нарушение кадровой политики и безопасности труда» включает:

3.1. нарушение трудового законодательства, результатом которого стало наложение на кредитную организацию санкций за нарушение норм трудового законодательства (выплаты работникам или бывшим работникам в виде компенсаций за нарушение условий трудового договора и (или) в связи с санкциями, наложенными исполнительным органом государственной власти, уполномоченным на осуществление федерального государственного надзора за соблюдением трудового законодательства);

3.2. нарушение норм безопасности и охраны труда, в том числе действия (бездействие) должностных лиц, результатом которых стали выплаты компенсаций работникам или бывшим работникам кредитной организации за причинение ущерба здоровью и (или) административных штрафов исполнительным органам государственной власти;

3.3. нарушения прав работников кредитной организации и третьих лиц, связанные с дискриминацией (половая, расовая, национальная дискриминация, а также дискриминация по языку, происхождению, имущественному и должностному положению, месту жительства, отношению

к религии, убеждениям, принадлежности к общественным объединениям и возрастному признаку).

4. Тип события операционного риска «нарушение прав клиентов и контрагентов» включает:

4.1. нарушение прав клиентов, состоящее в действиях со стороны кредитной организации, которые привели к несанкционированному раскрытию конфиденциальной информации, нарушению функционирования системы информационного обмена и взаимодействия с клиентом, повлекших 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 юрисдикцию которых попадают совершаемые операции, условий договоров на совершение операций, предоставление услуг, внутренних процедур кредитной организации взаимодействия с клиентами и контрагентами;

4.3. недостатки оказания услуг и проведения 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 кредитной организацией сопутствующих услуг. К данному типу событий операционного риска не относятся события, связанные с несовершенством и недостатками внутренних 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), произошедшими по вине кредитной организации, результатом которых стали претензии контрагентов и выплата им компенсаций.

5. Тип события операционного риска «ущерб материальным активам», включает события, связанные с природными и прочими внешними факторами, повлекшими досрочное списание (полное или частичное выбытие) материальных активов кредитной организации:

природные факторы, включая стихийные бедствия;

техногенные факторы;

социально-политические факторы;

медико-биологические факторы;

вандализм.

6. Тип события операционного риска «нарушение и сбои систем и оборудования» включает:

6.1. сбои в работе информационных систем и программного обеспечения, связанные с нарушением работоспособности технических средств и оборудования, объектов информационной инфраструктуры, программного обеспечения и других элементов информационных систем кредитной организации;

6.2. инфраструктурные сбои, состоящие в нарушении работы инфраструктуры (сбой систем кондиционирования, водоснабжения, электроснабжения), за исключением сбоев информационных систем и объектов информационной инфраструктуры, оказавших влияние на деятельность кредитной организации.

7. Тип события операционного риска «нарушение организации, исполнения и управления процессами кредитной организации» включает:

7.1. ошибки при подготовке, проведении и сопровождении операций, состоящие в нарушении внутренних процессов, стандартов, правил кредитной организации (например, к данному типу событий операционного риска относятся события операционного риска непреднамеренного характера, связанные с нарушением внутренних процедур проведения операций работниками кредитной организации (не связанные с преднамеренными действиями персонала), события операционного риска, связанные с

несовершенством и недостатками внутренних процессов, системы внутреннего контроля, систем управления рисками, недостатками распределения функций 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 отчетности;

7.3. ошибки при подготовке договоров и осуществлении 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 работы со средствами клиентов, находящимися в доверительном управлении;

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

7.6. ошибки кредитной организации, связанные с несоответствием внутренних документов кредитной организации законодательству Российской Федерации, нормативным актам исполнительных органов государственной власти, Банка России;

7.7. нарушения правил внутреннего контроля и процедур, установленных в кредитной организации в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения.

Приложение 5
к Положению Банка России
от 8 апреля 2020 года № 716-П
«О требованиях к системе управления операционным риском в кредитной организации и банковской группе»

Подходы к дополнительной классификации риска информационной безопасности

1. Кредитная организация (головная кредитная организация банковской группы) дополнительно классифицирует события риска информационной безопасности в разрезе типов событий нарушения защиты информации:

1.1. События риска информационной безопасности, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств:

получение оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, уведомлений в предусмотренной договором форме от клиентов – физических, юридических лиц, индивидуальных предпринимателей или лиц, занимающихся частной практикой, о случаях переводов денежных средств без согласия клиента, в том числе об использовании электронных средств платежа без согласия клиента;

получение расчетным центром платежной системы уведомлений от участников платежной системы о списании денежных средств с их корреспондентских счетов без их согласия и (или) с использованием искаженной информации, содержащейся в распоряжениях платежных клиринговых центров или участников платежной системы;

выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента, установленным Банком России и размещаемым на

официальном сайте Банка России в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»);

выявление оператором по переводу денежных средств, обслуживающим плательщика, включая оператора электронных денежных средств, операций по переводу денежных средств и операций по выдаче 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;

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

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

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

другие события нарушения защиты информации, связанные с несоблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств.

1.2. События риска информационной безопасности, связанные с неоказанием или несвоевременным оказанием услуг по переводу денежных средств:

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

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

невыполнение расчетным центром расчетов в течение операционного дня по принятым к исполнению распоряжениям платежного клирингового центра или участников платежной системы;

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

невыполнение платежным клиринговым центром в течение операционного дня платежного клиринга по принятым к исполнению распоряжениям участников платежной системы;

прерывание операционным центром предоставления операционных услуг на период более двух часов;

другие события риска информационной безопасности, связанные с неоказанием или несвоевременным оказанием услуг по переводу денежных средств.

1.3. События риска информационной безопасности, связанные с неоказанием или несвоевременным оказанием услуг:

неоказание услуг кредитной организацией на период более двух часов в целом по всем субъектам Российской Федерации, в которых кредитная организация предоставляет услуги;

неоказание услуг кредитной организацией на период более двух часов в целом по отдельным субъектам Российской Федерации, в которых кредитная организация предоставляет услуги;

другие события нарушения защиты информации, последствия или выявление которых могут привести к инциденту, связанному с неоказанием или несвоевременным оказанием услуг.

1.4. События риска информационной безопасности, связанные с нарушением требований к обеспечению защиты информации при осуществлении банковской деятельности, не связанные с переводами денежных средств:

получение уведомлений от клиентов – физических лиц, включая индивидуальных предпринимателей и (или) физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, и (или) юридических лиц о проведении банковской операции без их согласия;

выполнение банковских операций в результате несанкционированного доступа к объектам информационной инфраструктуры, данным и (или) информационным системам кредитной организации;

выявление кредитной организацией компьютерных атак, последствия от реализации которых могут привести к случаям и попыткам осуществления финансовой (банковской) операции без согласия клиента;

выявление фактов эксплуатации уязвимостей информационных систем, обусловленных ошибками и недостатками процессов обеспечения защиты информации кредитной организации;

другие события риска информационной безопасности, связанные с нарушением требований к обеспечению защиты информации при осуществлении банковской деятельности, не связанные с переводами денежных средств.

1.5. События риска информационной безопасности, связанные с обработкой (хранением, уничтожением) информации без использования

объектов информационной инфраструктуры и приводящие к утечке, искажению или потере информации конфиденциального характера (включая персональные данные), информации ограниченного доступа и других типов информации кредитной организации, не подлежащей разглашению или опубликованию, другим нарушениям.

2. Кредитная организация дополнительно классифицирует события риска информационной безопасности по источникам риска информационной безопасности в разрезе категорий источников операционного риска, приведенных в пункте 3.3 настоящего Положения.

2.1. По категории источников операционного риска «недостатки процессов»:

недостатки процессов применения кредитной организацией технологий обработки информации при осуществлении банковской деятельности, связанной с осуществлением перевода денежных средств, применяемых в отношении технологии обработки защищаемой информации, в соответствии с требованиями пункта 5 Положения Банка России № 683-П;

недостатки процессов применения кредитной организацией прикладного программного обеспечения автоматизированных систем и приложений, соответствующих требованиям к обеспечению защиты информации, приведенным в пункте 4 Положения Банка России № 683-П;

недостатки процессов проведения мероприятий, направленных на повышение качества системы управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности, в том числе процессов, реализующих уровни защиты информации в отношении объектов информационной инфраструктуры кредитной организации (головной кредитной организации банковской группы), установленные в соответствии с требованиями подпункта 3.1 пункта 3 Положения Банка России № 683-П;

недостатки других внутренних процессов, обеспечивающих функционирование системы обеспечения информационной безопасности кредитной организации.

2.2. По категории источников операционного риска «действия персонала и других связанных с кредитной организацией лиц» дополнительно выделяется реализация несанкционированного доступа персонала кредитной организации или третьих лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры кредитной организации (действия внутреннего нарушителя).

2.3. По категории источников операционного риска «сбои систем и оборудования» дополнительно выделяются сбои и отказы в работе прикладного программного обеспечения и приложений, а также объектов информационной инфраструктуры в результате реализации угроз безопасности информации.

2.4. По категории источников операционного риска «внешние причины» дополнительно выделяется реализация компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры кредитной организации (действия внешнего нарушителя), в том числе с целью:

блокирования штатного режима функционирования банковских или технологических процессов кредитной организации;

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. Более детализированные уровни классификации источников событий риска информационной безопасности определяются по видам процессов обеспечения мероприятий информационной безопасности в соответствии с подпунктом 2.1 настоящего пункта в зависимости от процессов кредитной организации, в которых они произошли.

2.6. В рамках дополнительной детализации классификации источников событий риска информационной безопасности кредитные организации подразделяют источники риска реализации угроз безопасности информации в разрезе направлений компьютерных атак, типов компьютерных атак и типов атакуемых объектов:

2.6.1. по направлениям компьютерных атак:

компьютерные атаки, направленные на объекты информационной инфраструктуры кредитной организации;

компьютерные атаки, 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 объектам информационной инфраструктуры кредитной организации;

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

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

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

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

компьютерные атаки, связанные с взаимодействием объектов информационной инфраструктуры кредитных организаций с центрами управления вредоносным программным обеспечением;

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 с оригиналом;

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 клиентом.

2.6.3.4. другой тип системы.

2.7. В случае если в процессе анализа риска информационной безопасности кредитной организацией (головной кредитной организацией

банковской группы) выявляются другие дополнительные источники события риска информационной безопасности, кредитная организация (головная кредитная организация банковской группы) определяет эти источники в базе событий.

3. В рамках дополнительной детализации классификации событий риска информационной безопасности в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, кредитная организация (головная кредитная организация банковской группы) осуществляет следующую детализацию классификации.

3.1. 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 автоматического устройства, конструкция которого предусматривает прием банкнот Банка России от клиентов и выдачу принятых банкнот Банка России клиентам без их обработки в кредитной организации, соответствующего требованиям, установленным Положением Банка России от 29 января 2018 года № 630-П «О порядке ведения кассовых операций и правилах хранения, перевозки и инкассации банкнот и монеты Банка России в кредитных организациях на территории Российской Федерации», зарегистрированным Министерством юстиции Российской Федерации 18 июня 2018 года № 51359;

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.

3.2. По технологическим участкам, определенным в пункте 5.2 Положения Банка России № 683-П.

4. Кредитная организация (головная кредитная организация банковской группы) использует следующие дополнительные (специфические) виды прямых и непрямых потерь от реализации риска информационной безопасности для классификации событий риска информационной безопасности в дополнение к установленным в пункте 3.11 настоящего Положения.

4.1. По категории «прямые потери» события риска информационной безопасности дополнительно классифицируются кредитной организацией (головной кредитной организацией банковской группы) следующие виды потерь:

потери денежных средств или других активов кредитной организации (головной кредитной организации банковской группы) в результате

реализации событий риска информационной безопасности, указанных в пункте 1 настоящего приложения;

выплаты компенсаций клиентам и контрагентам в результате реализации риска информационной безопасности, указанных в пункте 1 настоящего приложения;

уплата штрафов по предписаниям исполнительных органов государственной власти, Банка России и (или) администраторов платежных систем за реализацию риска информационной безопасности.

4.2. По категории «косвенные потери» кредитной организацией (головной кредитной организацией банковской группы) устанавливаются следующие виды потерь:

расчетные потери из-за приостановления и (или) прекращения функционирования объектов информационной инфраструктуры или потери ее работоспособности в результате реализации риска информационной безопасности;

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

рост стоимости договоров технического обслуживания объектов информационной инфраструктуры и (или) антивирусной защиты в результате реализации риска информационной безопасности.

4.3. По категории «качественные потери» кредитной организацией (головной кредитной организацией банковской группы) устанавливаются следующие виды потерь:

приостановление и (или) прекращение банковских процессов;

потеря работоспособности объектов информационной инфраструктуры;

нарушение целостности (искажение) или потеря данных;

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

другие потери качества объектов информационной инфраструктуры кредитной организации.