ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.3— 2022

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Издание официальное

Москва
Российский институт стандартизации
2023

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Центральным банком Российской Федерации (Банком России)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 122 «Стандарты финансовых операций»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 г. № 1548-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины и определения 3
4 Сокращения 8
5 Назначение и структура стандарта 8
6 Общие положения 9
7 Состав направлений, процессов и требований, определяемый комплексом стандартов 14
8 Требования к системе управления риском реализации информационных угроз 26
8.1 Общие положения 26
8.2 Направление 1 «Планирование системы управления риском реализации информационных угроз» 26
8.3 Направление 2 «Реализация системы управления риском реализации информационных угроз» 44
8.4 Направление 3 «Контроль системы управления риском реализации информационных угроз» . 54
8.5 Направление 4 «Совершенствование системы управления риском реализации информационных угроз» 60
Приложение А (обязательное) Классификация событий риска реализации информационных угроз с точки зрения источников риска 64
Приложение Б (обязательное) Классификация событий риска реализации информационных угроз и событий операционной надежности с точки зрения типов событий реализации информационных угроз 66
Приложение В (обязательное) Классификация событий риска реализации информационных угроз в разрезе видов (направлений) деятельности финансовых организаций 88
Приложение Г (обязательное) Классификация событий риска реализации информационных угроз в разрезе видов потерь от реализации риска 92
Приложение Д (обязательное) Состав КПУР для кредитных организаций 93
Приложение Е (обязательное) Состав КПУР для некредитных финансовых организаций 98
Библиография 100

Введение

Развитие и укрепление банковской системы Российской Федерации, развитие и обеспечение стабильности финансового рынка Российской Федерации и национальной платежной системы являются целями деятельности Банка России [1]. Одним из условий достижения этих целей является должная реализация процессов управления операционным риском, связанным с реализацией информационных угроз (далее — риск реализации информационных угроз), и обеспечение операционной надежности в условиях возможной реализации информационных угроз (далее — операционная надежность) в организациях финансового сектора — кредитных организациях, некредитных финансовых организациях Российской Федерации, а также субъектах национальной платежной системы[1)] (далее при совместном упоминании — финансовые организации), финансовых объединениях и экосистемах.

Негативные последствия от реализации информационных угроз в отдельных финансовых организациях, в том числе связанные с нарушением операционной надежности, в определенных случаях могут привести к быстрому развитию системного кризиса финансовых объединений и экосистем, а также банковской системы, финансового рынка Российской Федерации и (или) национальной платежной системы (далее при совместном упоминании — финансовая система), нанести существенный ущерб интересам собственников и многих клиентов финансовых организаций. Поэтому в условиях цифровой трансформации и ускоренного внедрения финансовыми организациями информационных и инновационных финансовых технологий управление риском реализации информационных угроз и обеспечение операционной надежности становятся для финансовых организаций важным аспектом их деятельности.

Надлежащее управление риском реализации информационных угроз и обеспечение операционной надежности наиболее актуально в рамках деятельности инфраструктурных организаций финансового рынка[2)], а также платежных систем, признанных значимыми в соответствии с нормативными актами Банка России [3]. Деятельность таких организаций ввиду их значимости и масштабов, сопровождается концентрацией на них множества рисков. Поэтому в отсутствие надлежащего управления рисками, включающего управление риском реализации информационных угроз, инфраструктурные организации финансового рынка и значимые платежные системы могут являться источниками и основным каналом распространения значимых в рамках финансовой системы рисков. В этой связи уровень обеспечения операционной надежности таких организаций может стать одним из решающих факторов для устойчивого функционирования финансовой системы [4].

Управление риском реализации информационных угроз для цели обеспечения операционной надежности в финансовых организациях является частью процесса управления операционным риском. При этом важно учитывать, что специфичные факторы, обусловленные возможностью реализации информационных угроз, в частности компьютерных атак, ставят новые задачи перед традиционными подходами к управлению операционным риском в финансовых организациях.

Следование принципу обеспечения «трех линий защиты», предполагающему выполнение действий в рамках непосредственного управления риском реализации информационных угроз «первой линией защиты», определение методологии, а также ее валидацию «второй линией защиты» и независимую оценку «третьей линией защиты», способствует интеграции системы управления таким риском в систему управления риском финансовой организации, в частности, систему управления операционным риском финансовой организации при ее наличии.

Одной из особенностей риска реализации информационных угроз является возможность применения нарушителем безопасности информации новых, ранее неизвестных сценариев реализации информационных угроз, в первую очередь, компьютерных атак путем скрытных, целенаправленных умышленных действий, которые в отличие от большинства других источников операционного риска вызывают трудности при их выявлении, устранении негативных последствий и установлении конечных масштабов негативного воздействия.

Разнообразный набор сценариев реализации компьютерных атак, создающих риск реализации

[1)] Субъекты национальной платежной системы, для которых определена актуальность вопросов управления риском реализации информационных угроз и обеспечения операционной надежности, определены в разделе 1 настоящего стандарта.

[2)] В рамках настоящего стандарта под инфраструктурными организациями финансового рынка понимаются организации, определенные в рамках нормативных актов Банка России [2] (финансовые организации, осуществляющие деятельность центрального контрагента, центрального депозитария, расчетного депозитария, репозитария).

информационных угроз, также осложняет управление таким риском. В результате наличия взаимосвязей и (или) взаимозависимостей между финансовыми организациями в рамках совместного выполнения отдельных бизнес- и технологических процессов, связанных с предоставлением финансовых и (или) информационных услуг, реализация компьютерных атак путем эксплуатации уязвимостей отдельных участников таких процессов может оказать негативное влияние на функционирование финансового объединения, финансовой экосистемы или финансовой системы в целом. При этом инфраструктурные организации финансового рынка могут послужить каналом для дальнейшего широкого распространения воздействия от реализации информационных угроз, в том числе компьютерных атак, например, вследствие распространения вредоносного кода среди организаций, с которыми они осуществляют взаимодействие.

Риск реализации информационных угроз, присущий взаимодействию финансовой организации с причастными сторонами, не обязательно связан со степенью их значимости. Любая финансовая организация может являться источником такого же риска реализации информационных угроз, как системно значимые финансовые организации, в случае если финансовая организация осуществляет активное взаимодействие с широким кругом участников финансовой системы, в том числе в рамках финансового объединения или экосистемы.

Среди возможных и наиболее опасных следует выделять сценарии реализации информационных угроз в результате действий внутреннего нарушителя безопасности информации. Реализация информационных угроз при таких сценариях может быть обусловлена как халатным отношением работников финансовой организации к соблюдению установленных требований к защите информации и обеспечению операционной надежности, так и совершением умышленных действий, в том числе по предварительному сговору с внешними участниками, приводящих к нарушению таких требований.

Компьютерные атаки могут обладать характеристиками скрытного и быстрого распространения, обусловленного наличием взаимосвязей и (или) взаимозависимостей в рамках информационного взаимодействия между объектами информатизации, а также быть связаны с эксплуатацией ранее неизвестных уязвимостей объектов информатизации и протоколов взаимодействия, а их реализация, в свою очередь, может приводить к нарушению функционирования объектов информатизации и (или) проникновению во внутренние вычислительные сети финансовых организаций, в том числе инфраструктурных организаций финансового рынка. Компьютерные атаки, связанные с эксплуатацией таких уязвимостей, нередко оказываются успешными несмотря на принятые меры защиты информации. Уменьшению негативного влияния в таком случае способствуют соответствующие меры, направленные на оперативное выявление, реагирование и восстановление функционирования бизнес- и технологических процессов и объектов информатизации после таких атак [4], [5].

Основными целями настоящего стандарта являются:

- определение перечня процессов системы управления риском реализации информационных угроз;

- определение требований к составу и содержанию мер по управлению риском реализации информационных угроз для уровней защиты, которые применяются финансовыми организациями в рамках планирования, реализации, контроля и совершенствования системы управления таким риском, а также систем управления, определенных в рамках семейства стандартов «Обеспечение операционной надежности» (далее — семейство стандартов ОН) и семейства стандартов «Защита информации финансовых организаций» (семейство стандартов ЗИ) комплекса национальных стандартов «Безопасность финансовых (банковских) операций»[1)]) (далее — комплекс стандартов).

- обеспечение возможности эффективного и стандартизированного контроля процессов системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов.

[1)] Разрабатывается Техническим комитетом по стандартизации ТК 122 «Стандарты финансовых операций».

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность финансовых (банковских) операций

УПРАВЛЕНИЕ РИСКОМ РЕАЛИЗАЦИИ ИНФОРМАЦИОННЫХ УГРОЗ И ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Общие положения

Security of financial (banking) operations.
Information threat risk management and ensuring operational resilience. General principles

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт определяет требования к составу и содержанию мер по управлению риском реализации информационных угроз для уровней защиты, которые применяются финансовыми организациями в рамках планирования, реализации, контроля и совершенствования системы управления таким риском, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов.

Настоящий стандарт служит для целей содействия соблюдению требований и рассматривается в качестве дополнения к нормативным актам Банка России, устанавливающим требования к системе управления операционным риском [6].

Положения настоящего стандарта предназначены для использования кредитными организациями, некредитными финансовыми организациями, указанными в части 1 статьи 76.1 Федерального закона [1].

Для отдельных субъектов национальной платежной системы — операторов услуг платежной инфраструктуры и операторов услуг информационного обмена, в целях снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы, а также надлежащего оказания услуг банкам и их клиентам рекомендуется применять меры в рамках следующих процессов системы управления риском реализации информационных угроз:

- выявление и идентификация риска реализации информационных угроз, а также его оценка;
- планирование, реализация, контроль и совершенствование комплекса мероприятий, направленных на повышение эффективности управления риском информационной безопасности и уменьшение негативного влияния риска информационной безопасности (далее — мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз);
- выявление событий риска реализации информационных угроз в части выявления и фиксации инцидентов, в том числе обнаружения компьютерных атак и выявления фактов (индикаторов) компрометации объектов информатизации;
- обеспечение осведомленности об актуальных информационных угрозах;
- установление и реализация программ контроля и аудита в части проведения сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз.

В соответствии с положениями нормативных актов Банка России положения настоящего стандарта могут применяться иными организациями, реализующими инновационные бизнес- и технологические процессы, связанные с предоставлением финансовых, банковских услуг, в том числе услуг по осуществлению переводов денежных средств (далее при совместном упоминании — финансовые услуги) и (или) информационных услуг.

Издание официальное

Состав мер по управлению риском реализации информационных угроз, определяемый настоящим стандартом, применим в рамках осуществления видов деятельности финансовой организации[1)], связанных с предоставления финансовых и (или) информационных услуг, в отношении элементов критичной архитектуры, идентифицируемой в рамках процесса, предусмотренного в рамках семейств стандартов ОН.

Область применения настоящего стандарта, определяющая обязанность финансовых организаций применять меры управления риском реализации информационных угроз, реализующие один из уровней защиты в рамках осуществления видов деятельности финансовой организации, связанных с осуществлением финансовых и (или) информационных услуг, устанавливается в нормативных актах Банка России путем включения нормативной ссылки на настоящий стандарт, приводимой на основании статьи 27 Федерального закона [7].

Настоящий стандарт применяется путем включения нормативных ссылок на него в нормативных актах Банка России и (или) прямого использования устанавливаемых в нем требований во внутренних документах финансовых организаций, а также в договорах.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 51897/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения

ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 57580.1—2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер

ГОСТ Р 57580.2 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 57580.4—2022 Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ГОСТ Р ИСО/МЭК 17021-1 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента. Часть 1. Требования

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО/МЭК 27006 Информационные технологии. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27036-2 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования

ГОСТ Р ИСО/МЭК 27036-4 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Рекомендации по обеспечению безопасности облачных услуг

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт,

[1)] Для кредитных организаций вместо видов деятельности следует рассматривать направления деятельности, определенные в соответствии с нормативными актами Банка России [6].

на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **бизнес-процесс и (или) технологический процесс финансовой организации; бизнес- и технологический процесс:** Набор взаимосвязанных операций, в том числе технических, в отношении активов финансовой организации или информации и (или) объектов информатизации, используемых при осуществлении финансовой организацией видов деятельности, связанных с предоставлением финансовых и (или) информационных услуг.

Примечание — Адаптировано из ГОСТ Р 57580.1.

3.2 **объект информатизации (прикладного и инфраструктурного уровней финансовой организации); объект информационной инфраструктуры:** Совокупность объектов и ресурсов доступа, средств и систем обработки информации, используемых для обеспечения информатизации бизнес- и технологических процессов финансовой организации, используемых для предоставления финансовых и (или) информационных услуг.

Примечание — Адаптировано из ГОСТ Р 57580.1.

3.3 **критичный актив:** Объект информатизации, субъект доступа, а также защищаемая информация[1)], подготавливаемая, передаваемая, обрабатываемая и (или) хранимая в рамках выполнения бизнес- и технологических процессов, воздействие на которые и (или) нарушение функционирования которых может привести к превышению пороговых значений контрольных показателей уровня риска реализации информационных угроз[2)] и целевых показателей операционной надежности.

3.4 **информационная угроза; угроза безопасности информации:** Совокупность условий и факторов, побуждающих клиента финансовой организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотреблением доверием, и (или) создающих возможность нарушения безопасности информации, вызывающую или способную вызвать негативные последствия (включая нарушение операционной надежности) для финансовой организации, причастных сторон, в том числе клиентов финансовой организации.

Примечания

1 Адаптировано из ГОСТ Р 53114.

2 К негативным последствиям реализации информационных угроз относятся:

возникновение потерь финансовой организации, причастных сторон, в том числе клиентов финансовой организации, а также иных третьих лиц;

нарушение операционной надежности финансовой организации;

невыполнение обязательств по обеспечению защиты интересов клиентов финансовой организации;

несоблюдение требований законодательства Российской Федерации в области защиты информации, устанавливаемых на основании статей 57.4 и 76.4-1 Федерального закона [1], части 3 статьи 27 Федерального закона [11], а также устанавливаемых статьей 19 Федерального закона [12], статьей 16 Федерального закона [13] и Федеральным законом [14].

3 Киберугрозы являются одним из видов информационных угроз.

3.5 **источник риска реализации информационных угроз:** Объект или деятельность, которые самостоятельно или в комбинации с другими обладают возможностью вызывать или повышать уровень риска реализации информационных угроз.

Примечание — Адаптировано из ГОСТ Р ИСО 31000.

---

1) К защищаемой информации относится информация, перечень которой определен в [8]—[10].

2) В том числе превышение целевых показателей операционной надежности, устанавливаемых в соответствии с требованиями нормативных актов Банка России.

3.6 **компьютерная атака:** Вид информационной угрозы, заключающейся в преднамеренных действиях со стороны работников финансовой организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, в том числе штатных, направленных на критичные активы.

3.7 **уязвимость:** Недостаток применения технологических мер защиты информации, применяемых объектов информатизации прикладного уровня, недостаток планирования, реализации, контроля и совершенствования процессов управления риском реализации информационных угроз, обеспечения операционной надежности и (или) защиты информации, эксплуатация которого позволяет нарушителю безопасности информации реализовать информационные угрозы в отношении критичных активов.

3.8 **риск реализации информационных угроз; информационной безопасности:** Возможность реализации информационных угроз (в совокупности с последствиями от их реализации), которые обусловлены недостатками процессов обеспечения операционной надежности и защиты информации, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности финансовой организации.

Примечание — Риск реализации информационных угроз включает в себя:

киберриск — риск преднамеренных действий со стороны работников финансовой организации и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информатизации финансовой организации 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;

другие виды риска реализации информационных угроз, связанные с обработкой (хранением, уничтожением) информации без использования объектов информатизации, а также связанные со случаями побуждения клиентов финансовой организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотребления доверием (методов социальной инженерии), которые привели и (или) могут привести к случаям мошенничества и (или) кражи с банковского счета в отношении клиентов финансовой организации.

3.9 **ключевой индикатор риска реализации информационных угроз;** КИР: Количественный показатель, используемый для оперативного измерения и контроля уровня риска реализации информационных угроз в определенный момент времени.

3.10 **контрольный показатель уровня риска реализации информационных угроз; контрольный показатель риска информационной безопасности;** КПУР: Количественный или качественный показатель, определяемый во внутренних документах финансовой организации на плановый годовой период в целях контроля за уровнем риска реализации информационных угроз.

3.11 **сигнальное значение КПУР:** Предельное значение, нарушение которого является сигналом о необходимости ежедневного мониторинга значений и оперативной реализации мер, направленных на снижение риска реализации информационных угроз.

3.12 **контрольное значение КПУР:** Предельное значение, нарушение которого является сигналом о необходимости принятия действий в рамках корпоративного управления, в том числе в рамках системы управления риском финансовой организации, таких как информирование совета директоров (наблюдательного совета), изменение политики управления риском реализации информационных угроз.

3.13 **инцидент (связанный с реализацией информационных угроз):** Одно или серия связанных нежелательных событий, связанных с возможной реализацией информационных угроз, которые указывают на свершившуюся, предпринимаемую или вероятную реализацию информационных угроз.

Примечания

1 К инцидентам, связанным с реализацией информационных угроз, относятся:

киберинциденты — инциденты, связанные с реализацией информационных угроз, в результате компьютерных атак;

другие инциденты, связанные с реализацией информационных угроз при обработке (хранении, уничтожении) информации без использования объектов информатизации, а также связанные со случаями побуждения клиентов финансовой организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотребления доверием (методов социальной инженерии), которые привели и (или) могут привести к фактам мошенничества и (или) кражи с банковского счета в отношении клиентов финансовой организации.

2 Адаптировано из ГОСТ Р 57580.1.

3.14 **событие, связанное с возможной реализацией информационных угроз; событие реализации информационных угроз:** Идентифицированное возникновение и (или) изменение состояния объектов информатизации финансовой организации, действия работников финансовой организации и (или) иных лиц, указывающие на возможный инцидент, связанный с реализацией информационных угроз.

Примечание — К событиям, связанным с возможной реализацией информационных угроз, относятся:

киберсобытия — события реализации информационных угроз, указывающие на возможный киберинцидент;

другие события реализации информационных угроз, указывающие на возможный инцидент, связанный с реализацией информационных угроз при обработке (хранении, уничтожении) информации без использования объектов информатизации, а также указывающие на возможный инцидент, связанный со случаями побуждения клиентов финансовой организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотребления доверием (методов социальной инженерии), которые привели и (или) могут привести к фактам мошенничества и (или) кражи с банковского счета в отношении клиентов финансовой организации.

3.15 **событие риска (реализации информационных угроз); событие риска информационной безопасности:** Инцидент, связанный с реализацией информационных угроз, который привел к фактической реализации риска реализации информационных угроз, вследствие чего возникли прямые и непрямые потери финансовой организации.

3.16 **управление риском реализации информационных угроз**: Скоординированные действия по руководству и управлению деятельностью финансовой организации и взаимодействию с причастными сторонами в связи с риском реализации информационных угроз.

Примечания

1 Адаптировано из ГОСТ Р 53114.

2 Управление риском реализации информационных угроз в кредитных организациях должно быть направлено на общее управление рисками (в рамках системы управления рисками и капиталом), в значении, установленном нормативными актами Банка России [15].

3.17 **система управления риском реализации информационных угроз:** Совокупность процедур (процессов, требований и мер), применение которых направлено на обеспечение эффективности процессов управления риском реализации информационных угроз путем планирования, реализации, контроля и совершенствования таких процессов.

3.18 **область применения системы управления риском реализации информационных угроз; критичная архитектура:** Совокупность бизнес- и технологических процессов, критичных активов финансовой организации, включая их взаимосвязи и взаимозависимости.

3.19 **аутсорсинг:** Передача финансовой организацией на основании договора на длительный срок (например, от одного года) сторонней (внешней) организации — поставщику услуг выполнения бизнес- и технологических процессов финансовой организации, которые являются необходимыми для ее деятельности и которые в обычных условиях (без привлечения поставщика услуг) осуществлялись бы финансовой организацией самостоятельно.

3.20 **поставщик услуг [информационных сервисов и услуг]:** Обслуживающая организация, специализирующаяся на предоставлении информационных сервисов и услуг, в том числе в рамках которых финансовые организации передают выполнение своих бизнес- и технологических процессов на аутсорсинг.

Примечания

1 Поставщиком услуг (в том числе поставщиком облачных услуг) может выступать как аффилированное в пределах финансовой организации юридическое лицо, так и физическое или юридическое лицо, которое является внешним по отношению к финансовой организации (в том числе как потребителя облачных услуг), привлекаемым для выполнения на постоянной (непрерывной) основе определенных бизнес- и технологических процессов финансовой организации, выполнение которых в обычных условиях (без привлечения поставщика услуг) осуществлялось бы финансовой организацией самостоятельно.

2 Термин «поставщик облачных услуг» используется в значении, применяемом в ГОСТ Р ИСО/МЭК 27036-4.

3.21 **уровень защиты:** Определенная совокупность мер управления риском реализации информационных угроз, входящих в состав системы управления таким риском, а также мер, входящих в состав систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов,

применяемых совместно в пределах области применения указанных систем, в том числе с целью реализации положений нормативных актов Банка России.

3.22 **технологические меры защиты информации:** Меры, направленные на обеспечение безопасности технологии обработки защищаемой информации[1)].

3.23 **клиент — потребитель финансовых и (или) информационных услуг финансовой организации; клиент финансовой организации:** Юридическое или физическое лицо, являющееся конечным потребителем финансовых и (или) информационных услуг финансовой организации.

3.24 **внешний аудит процессов обеспечения операционной надежности и защиты информации; аудит:** Независимый и документируемый процесс получения свидетельств в рамках оценки уровней зрелости процессов обеспечения операционной надежности и защиты информации и соответствия уровней зрелости соответствующих процессов принятым финансовой организацией значениям КПУР, проводимый внешней, независимой по отношению к проверяемой, проверяющей организацией.

3.25 **внутренний нарушитель (безопасности информации):** Лицо, в том числе работник финансовой организации, работник поставщиков услуг, реализующее информационные угрозы с использованием легально предоставленных им прав доступа, в том числе с использованием уязвимостей.

3.26 **риск внутреннего нарушителя:** Риск реализации информационных угроз, обусловленный наличием возможности совершения действий в отношении критичных активов со стороны внутреннего нарушителя.

3.27 **внешний нарушитель (безопасности информации):** Лицо, реализующее информационные угрозы без использования легально предоставленных прав доступа, с использованием уязвимостей.

3.28 **операционная надежность (в условиях возможной реализации информационных угроз); киберустойчивость:** Способность финансовой организации обеспечивать непрерывность функционирования бизнес- и технологических процессов (3.1) с учетом целевых показателей операционной надежности в условиях возможной реализации информационных угроз.

Примечания

1 В настоящем стандарте рассматривается частный случай определения операционной надежности.

2 В настоящем стандарте термин «операционная надежность» используется в значении, определяющем свойства осуществляемых финансовой организацией видов деятельности, связанных с предоставлением финансовых и (или) информационных услуг.

3.29 **финансовая экосистема:** Совокупность пользователей, поставщиков финансовых услуг, поставщиков услуг в сфере информационных технологий, обеспечивающих функционирование финансовой экосистемы, а также техническое и технологическое сопровождение предоставления финансовых услуг в рамках финансовой экосистемы (далее — поставщики услуг в сфере информационных технологий); политик, требований и правил, обеспечивающих доступность и безопасность предоставляемых в рамках финансовой экосистемы финансовых и (или) информационных услуг.

Примечания

1 Пользователь финансовой экосистемы: юридическое или физическое лицо, являющееся конечным потребителем финансовых и (или) информационных услуг, предоставляемых в рамках финансовой экосистемы;

поставщик финансовых услуг: кредитные организации, некредитные финансовые организациями, указанные в части 1 статьи 76.1 Федерального закона [1], а также отдельные субъекты национальной платежной системы, предоставляющие финансовые и (или) информационные услуги с применением информационных технологий, реализуемых в рамках финансовой экосистемы;

поставщики услуг в сфере информационных технологий: обслуживающая организация, специализирующаяся на предоставлении информационных сервисов и услуг, обеспечивающих функционирование финансовой экосистемы, а также техническое и (или) технологическое сопровождение предоставления финансовых и (или) информационных услуг в рамках финансовой экосистемы.

2 В большинстве случаев деятельность финансовых экосистем является значимой в рамках финансовой системы, так как распространяется на широкий круг пользователей, оказывая влияние на показатели финансовой системы, характеризующие ее экономическое состояние, стабильность, а также финансовую доступность для потребителей финансовых и (или) информационных услуг.

3.30 **причастная сторона (финансовой организации):** Лицо, группа лиц или организация, которые могут воздействовать на риск реализации информационных угроз, подвергаться воздействию

[1)] К защищаемой информации относится информация, перечень которой определен в [8]—[10].

или ощущать себя подверженными воздействию такого риска в рамках взаимодействия с финансовой организацией, в том числе связанного с предоставлением финансовых и (или) информационных услуг.

Примечания

1 В настоящем стандарте к причастным сторонам финансовой организации следует относить клиентов финансовой организации, а также следующие организации:

а) другие финансовые организации, участвующие в выполнении бизнес- и технологических процессов финансовой организации (включая инфраструктурные организации финансового рынка), в том числе входящие в состав финансового объединения или финансовой экосистемы;

б) поставщики услуг (3.20), в том числе поставщики облачных услуг, а также организации, осуществляющие поставку программных и (или) аппаратных продуктов, в том числе разрабатываемых по заказу;

в) иные контрагенты финансовой организации: поставщики коммунальных услуг, поставщики телекоммуникационных услуг общего пользования.

2 Адаптировано из ГОСТ 51897.

3.31 **служба информационной безопасности;** служба ИБ: Специализированное подразделение (работники), ответственное (ответственные) за организацию и контроль обеспечения безопасности информации.

3.32 **центры компетенции:** Подразделения финансовой организации, осуществляющие в рамках системы управления риском реализации информационных угроз сбор информации и информирование о выявленном риске, оценку выявленных рисков (в пределах своей компетенции), разработку и внедрение мероприятий, направленных на уменьшение негативного влияния риска, и мониторинг уровня риска в своих процессах.

Примечание — К центрам компетенции в рамках системы управления риском реализации информационных угроз относятся подразделения, 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 (подразделения), ответственные за осуществление операций и сделок и за результаты процесса, и подразделения, обеспечивающие процессы финансовой организации.

3.33 **уровень зрелости:** Показатель, характеризующий степень развития в финансовой организации системы управления риском реализации информационных угроз, процессов обеспечения операционной надежности и защиты информации, включая процессы применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов, и реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня.

Примечания

1 Определение уровня зрелости системы управления риском реализации информационных угроз осуществляется в отношении такой системы целиком согласно методике оценки зрелости, приводимой в рамках семейства стандартов УР «Управление риском реализации информационных угроз и обеспечение операционной надежности» Комплекса стандартов.

2 Определение уровня зрелости процессов обеспечения операционной надежности и защиты информации осуществляется согласно методикам оценки соответствия, приводимым в рамках семейств стандартов ОН и ЗИ комплекса стандартов соответственно.

3 Определение уровня зрелости процессов применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов, и реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня, в отношении которых требуется проведение сертификации в системе сертификации[1)] или проведение оценки соответствия по требованиям к оценочному уровню доверия не ниже, чем ОУД 4, в соответствии с требованиями ГОСТ Р ИСО/МЭК 15408-3, осуществляется в соответствии с нормативными актами Банка России.

3.34 **служба управления рисками:** Подразделение (работники), ответственное (ответственные) за осуществление функций и (или) организацию системы управления рисками финансовой организации.

[1)] Система сертификации федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченным органом в области экспортного контроля.

Примечание — В целях организации управления операционным риском в финансовой организации рекомендуется (в случае если создание такого подразделения не предусмотрено нормативными актами Банка России [6]) создание соответствующего подразделения, структурно входящего в службу управления рисками.

3.35 **подразделение, уполномоченное проводить оценку эффективности системы управления риском реализации информационных угроз; уполномоченное подразделение:** Подразделение (работники), структурно независимое (независимые) от службы ИБ и службы управления рисками, уполномоченное (уполномоченные) проводить оценку эффективности функционирования системы управления риском реализации информационных угроз, в том числе оценку полноты и качества выполнения мероприятий, направленных на уменьшение негативного влияния от риска реализации информационных угроз (например, служба внутреннего аудита).

Примечание — В соответствии с требованиями нормативных актов Банка России на уполномоченное подразделение могут возлагаться иные функции [6], в частности проверка соблюдения требований нормативных актов Банка России.

3.36 **политика, определяющая подходы к управлению риском реализации информационных угроз; политика управления риском реализации информационных угроз; политика информационной безопасности:** Общее намерение и направление, официально устанавливаемое советом директоров (наблюдательным советом) или коллегиальным исполнительным органом[1)] финансовой организации.

Примечания

1 Адаптировано из ГОСТ Р ИСО/МЭК 27002.

2 Способ документарного определения политики управления риском реализации информационных угроз финансовые организации определяют самостоятельно.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

БЛ — банковская лицензия;

НКО — небанковская кредитная организация;

НСД — несанкционированный доступ;

ОПДС — оператор по переводу денежных средств;

ПО — программное обеспечение;

СВР — степень возможности реализации;

СТП — степень тяжести последствий;

УЛ — универсальная лицензия.

5 Назначение и структура стандарта

Настоящий стандарт является базовым в рамках комплекса стандартов и исходит из парадигмы, что для обеспечения должного уровня операционной надежности и защиты информации, для возможности противостоять реализации информационных угроз в виде событий риска реализации информационных угроз финансовым организациям следует обеспечивать планирование, реализацию, контроль и совершенствование следующих систем (с учетом структуры и взаимосвязей, приведенных на рисунке 2):

- системы управления риском реализации информационных угроз, определенной в рамках настоящего стандарта, формирующего основу семейства стандартов УР «Управление риском реализации информационных угроз и обеспечение операционной надежности»;
- системы организации и управления защитой информации, определенной в рамках семейства стандартов ЗИ;

[1)] В зависимости от реализуемого финансовой организацией уровня защиты, а также требований нормативных актов Банка России [6].

- системы организации и управления операционной надежностью, определенной в рамках семейства стандартов ОН.

Структура комплекса стандартов приведена на рисунке 1.

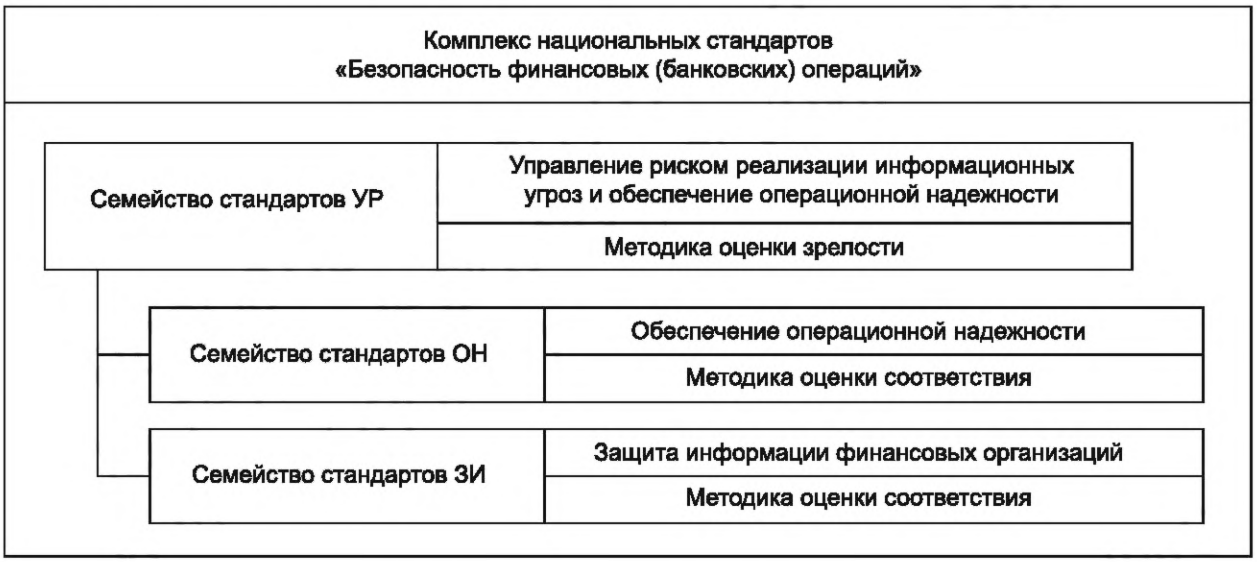

Рисунок 1 — Структура комплекса стандартов

Раздел 6 «Общие положения» настоящего стандарта содержит:

- общие положения и рекомендации по реализации финансовой организацией системы управления риском реализации информационных угроз;
- описание подхода к интеграции системы управления риском реализации информационных угроз в систему управления рисками финансовой организации.

Раздел 7 «Состав направлений, процессов и требований, определяемый комплексом стандартов» настоящего стандарта определяет состав направлений, процессов и требований по управлению риском реализации информационных угроз и обеспечению операционной надежности (семейство стандартов УР), обеспечению операционной надежности (семейство стандартов ОН), защите информации финансовых организаций (семейство стандартов ЗИ).

Раздел 8 «Требования к системе управления риском реализации информационных угроз» настоящего стандарта содержит для каждого уровня защиты описание состава мер, направленных на реализацию требований к процессам в рамках планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз.

6 Общие положения

6.1 Деятельности финансовой организации свойственен риск реализации информационных угроз, что является объективной реальностью, и понизить этот риск можно лишь до определенного остаточного уровня.

Для управления риском реализации информационных угроз финансовой организации необходимо обеспечить планирование, реализацию, контроль и совершенствование системы управления риском реализации информационных угроз.

Примечание — По решению финансовой организации могут быть созданы отдельные системы управления в целях управления отдельным видом риска реализации информационных угроз (согласно примечанию к 3.8).

Эффективное управление риском реализации информационных угроз должно начинаться с определения структуры и организации системы управления таким риском, а также политики, которая устанавливает приоритеты в вопросах управления риском реализации информационных угроз для достижения целей операционной надежности.

6.2 Вопросы управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации должны учитываться при принятии решений, связанных с общей

стратегией развития бизнеса финансовой организации. Должна также учитываться значимость ресурсов (кадровых и финансовых), необходимых для обеспечения должного уровня зрелости процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации.

6.3 Выполнение процессов системы управления риском реализации информационных угроз должно способствовать обеспечению операционной надежности финансовой организации применительно к совокупности бизнес- и технологических процессов, критичных активов — объектов информатизации прикладного и инфраструктурного уровней, субъектов доступа и защищаемой информации.

Примечание — В настоящем стандарте объекты информатизации подразделяются на объекты информатизации прикладного и инфраструктурного уровня.

К объектам информатизации инфраструктурного уровня относятся объекты информатизации следующих системных уровней:

- уровня аппаратного обеспечения;
- уровня сетевого оборудования;
- уровня сетевых приложений и сервисов;
- уровня операционных систем, систем управления базами данных, серверов приложений.

К объектам информатизации прикладного уровня относятся объекты информатизации следующих уровней:

а) уровня автоматизированных систем и приложений, эксплуатируемых для оказания финансовых услуг в рамках бизнес- и технологических процессов финансовой организации, в том числе:

- система дистанционного банковского обслуживания;
- система обработки транзакций;
- информационные ресурсы сети Интернет;
- автоматизированная банковская система;
- система посттранзакционного обслуживания операций;
- автоматизированные системы, в том числе информационно-аналитические системы, используемые финансовой организацией;
- сервисы, предоставляемые поставщиками облачных услуг;

б) уровня автоматизированных систем и приложений, эксплуатируемых клиентом финансовой организации при пользовании финансовыми (банковскими) и (или) информационными услугами.

Критичные активы финансовой организации обладают разной степенью значимости для осуществления видов деятельности отдельной финансовой организации (в том числе для выполнения бизнес- и технологических процессов), а также в разной степени подвержены воздействию информационных угроз. Финансовой организации следует применять риск-ориентированный подход при определении приоритетов по реализации мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз таким образом, чтобы реализуемые мероприятия были адекватны и оптимальны.

6.4 Выполнение процессов системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ЗИ и ОН комплекса стандартов, должно обеспечивать достижение следующих целей:

- обеспечение операционной надежности финансовой организации;
- обеспечение соответствия фактического уровня риска реализации информационных угроз, контроль которого также осуществляется со стороны подразделений, формирующих «вторую» и «третью линии защиты», допустимому, принятому финансовой организацией в соответствии с принятыми значениями КПУР;
- надлежащая интеграция системы управления риском реализации информационных угроз в систему управления рисками финансовой организации в составе операционного риска;
- оперативное реагирование и адаптация к изменению информационных угроз, присущих как выполнению внутренних процессов финансовой организации, так и ее внешнему взаимодействию.

6.5 Интеграция системы управления риском реализации информационных угроз в систему управления рисками финансовой организации осуществляется посредством управления риском реализации информационных угроз как одним из видов операционного риска.

Надлежащая интеграция системы управления риском реализации информационных угроз в систему управления операционным риском финансовой организации достигается:

а) интеграцией процессов системы управления риском реализации информационных угроз в состав процессов управления операционным риском, включая:

- выявление и идентификацию риска реализации информационных угроз, а также его оценку;
- планирование, реализацию, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз;
- сбор и регистрацию информации о внутренних событиях риска реализации информационных угроз и потерях;
- мониторинг риска реализации информационных угроз;
- оценку эффективности функционирования системы управления риском реализации информационных угроз;
- организацию внутренней отчетности в рамках управления риском, в том числе в целях информирования совета директоров (наблюдательного совета) и исполнительного органа финансовой организации о фактическом уровне такого риска (как составной части операционного риска);
- оценку капитала, необходимого на покрытие риска реализации информационных угроз (как составной части операционного риска), а также организация внутренней отчетности о его достаточности[1)];

б) следованием принципу «трех линий защиты» в рамках управления риском реализации информационных угроз (как составной частью операционного риска), а также созданием условий для реализации каждой «линией защиты» своих функций, в том числе:

- выделение необходимого ресурсного (кадрового и финансового) обеспечения;
- распределение функций, ролей и ответственности среди вовлеченных подразделений (работников), формирующих «три линии защиты»;
- регулярное обучение и повышение квалификации вовлеченных работников;
- развитие корпоративной этики (культуры), устанавливающей значимость управления рисками, в том числе риском реализации информационных угроз;
- определение механизмов для взаимодействия между «линиями защиты» в рамках выполнения их функций.

Примечания

1 В качестве примера в настоящем стандарте используется следующее распределение подразделений (работников) финансовой организации согласно принципу «трех линий защиты»:

- «первая линия защиты»: центры компетенции;
- «вторая линия защиты»: служба управления рисками (в том числе подразделение, ответственное за организацию управления операционным риском), служба ИБ;
- «третья линия защиты»: уполномоченное подразделение.

2 Для выполнения функций в рамках каждой «линии защиты» могут привлекаться не одно, а несколько структурных подразделений финансовой организации;

в) интеграцией подходов к организации контроля за уровнем риска реализации информационных угроз в составе операционного риска:

- определения и установления состава, а также пороговых значений КИР, в том числе согласно требованиям нормативных актов Банка России [6], с целью оперативного мониторинга фактического уровня риска реализации информационных угроз;
- определения и установления состава, а также сигнальных и контрольных значений КПУР (в том числе согласно требованиям нормативных актов Банка России [6]);
- определения способов возмещения запланированных (ожидаемых)[2)] и незапланированных (реализация стрессового сценария)[3)] потерь от риска реализации информационных угроз, в том числе расчет капитала, необходимого на покрытие таких потерь[4)];
- классификации событий риска реализации информационных угроз, по источникам риска реализации информационных угроз, типам событий реализации информационных угроз, видам (направлениям) деятельности (в том числе бизнес- и технологическим процессам) финансовой организации, видам

---

1) В случае если соответствующие требования установлены нормативными актами Банка России [6].

2) Определяемые на основе данных внутренней отчетности о фактических потерях за определенный временной период.

3) Определяемые на основе оценки возможных потерь в маловероятных, но стрессовых сценариях.

4) В случае если соответствующие требования установлены нормативными актами Банка России [6].

потерь финансовой организации, ее причастных сторон, в том числе клиентов финансовой организации (в том числе согласно требованиям нормативных актов Банка России [6]);

- реализации и ведения на постоянной основе аналитической базы данных о событиях риска реализации информационных угроз, в том числе согласно требованиям нормативных актов Банка России [6] (далее — база событий риска реализации информационных угроз).

Примечание — По решению финансовой организации аналитическая база данных о событиях риска реализации информационных угроз может вестись как отдельно, так и в рамках аналитической базы событий операционного риска;

- организации оперативного мониторинга значений КИР с целью принятия оперативных решений по управлению риском реализации информационных угроз, а также накопления статистических данных (в том числе согласно требованиям нормативных актов Банка России [6]);
- контроля соблюдения установленных значений КПУР с целью контроля уровня риска реализации информационных угроз, в том числе в части обеспечения соблюдения требований по достаточности капитала, необходимого на покрытие запланированных и незапланированных потерь от риска реализации информационных угроз[1)];
- учета фактических значений КПУР при определении способов покрытия запланированных и незапланированных потерь от риска реализации информационных угроз, в том числе при расчете капитала, необходимого на покрытие таких потерь[1)];
- валидации и верификации со стороны подразделения, формирующих «третью линии защиты», методологии, данных и внутренней отчетности в рамках управления риском реализации информационных угроз[2)].

6.6 Операционная надежность финансовой организации характеризуется:

- способностью финансовой организации обеспечивать необходимый уровень зрелости процессов обеспечения операционной надежности и защиты информации согласно принятым финансовой организацией значениям КПУР;
- способностью финансовой организации обеспечить покрытие собственных потерь, потерь причастных сторон, в том числе клиентов финансовой организации, в результате инцидентов, в том числе за счет формирования финансового резерва и (или) страхования риска реализации информационных угроз.

Примечание — В случае если требованиями нормативных актов Банка России не предусмотрено формирование резервов на покрытие потерь от реализации операционного риска, финансовые организации самостоятельно определяют способы покрытия потерь в результате инцидентов;

- способностью финансовой организации обеспечить выполнение обязательств по защите интересов клиентов финансовой организации;
- способностью финансовой организации осуществлять финансовые (банковские) операции, в том числе операции по переводу денежных средств, в рамках срока исполнения обязательств, а также обеспечивать завершенность расчетов по таким операциям согласно установленному режиму работы;
- способностью финансовой организации возобновить предоставление финансовых и (или) информационных услуг в течение установленного времени после нарушения в работе в результате инцидентов;
- способностью финансовой организации обеспечить соблюдение требований законодательства Российской Федерации в области защиты информации, устанавливаемых на основании статьей 57.4 и 76.4-1 Федерального закона [1], части 3 статьи 27 Федерального закона [11], а также устанавливаемых статьей 19 Федерального закона [12], статьей 16 Федерального закона [13] и Федеральным законом [14].

6.7 Настоящий стандарт определяет три уровня защиты:

- уровень 3 — минимальный;
- уровень 2 — стандартный;
- уровень 1 — усиленный.

---

1) В случае если соответствующие требования установлены нормативными актами Банка России [6].

2) Осуществляется посредством ежегодной оценки эффективности функционирования системы управления риском реализации информационных угроз (проводимой в составе оценки эффективности функционирования системы управления операционным риском).

Уровень защиты для финансовой организации устанавливается нормативными актами Банка России на основе:

- вида деятельности финансовой организации, состава предоставляемых финансовой организацией услуг, реализуемых бизнес- и технологических процессов;
- объема финансовых (банковских) операций, в том числе операций по переводу денежных средств;
- размера организации, отнесения финансовой организации к категории малых предприятий и микропредприятий;
- значимости и роли финансовой организации в рамках банковской системы, финансового рынка Российской Федерации и (или) национальной платежной системы.

6.8 Планирование системы управления риском реализации информационных угроз включает:

- определение политики управления риском реализации информационных угроз;
- выявление и идентификацию риска реализации информационных угроз, а также его оценку;
- организацию ресурсного (кадрового и финансового) обеспечения.

6.9 Реализация системы управления риском реализации информационных угроз включает:

- планирование, реализацию, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз:

разработку мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз;

защиту от информационных угроз;

реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации;

- выявление событий риска реализации информационных угроз;
- обеспечение осведомленности об актуальных информационных угрозах.

6.10 Контроль системы управления риском реализации информационных угроз включает:

- установление и реализацию программ контроля и аудита;
- мониторинг риска реализации информационных угроз.

6.11 Совершенствование системы управления риском реализации информационных угроз включает обеспечение соответствия фактических значений КПУР принятым.

6.12 Способность финансовой организации распознавать признаки возможного инцидента имеет важное значение для обеспечения операционной надежности.

Раннее обнаружение инцидентов позволяет финансовой организации оперативно принять соответствующие меры реагирования (контрмеры), позволяющие сдержать или парировать фактическую реализацию таких инцидентов. В свою очередь, оперативное принятие мер реагирования (контрмер) в большинстве случаев позволяет свести к минимуму негативные последствия от реализации таких инцидентов.

В целях снижения возможности возникновения системных рисков невыполнения обязательств перед причастными сторонами финансовой организации следует проектировать и реализовывать свои бизнес- и технологические процессы способом, обеспечивающим быстрое и безопасное возобновление предоставления финансовых и (или) информационных услуг, а также корректное и полное восстановление данных о совершенных финансовых (банковских) операциях, в том числе операциях по переводу денежных средств.

6.13 Осведомленность об актуальных информационных угрозах способствует корректному определению финансовой организацией модели информационных угроз в контексте ее видов деятельности, связанных с предоставлением финансовых и (или) информационных услуг, в том числе их влияния на осуществление таких видов деятельности, а также полноты и качества реализуемых мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз.

Достижению высокого уровня осведомленности об актуальных информационных угрозах способствует проведение анализа (исследования) возможных информационных угроз и проведение систематических работ по поиску соответствующей информации. Осведомленность об актуальных информационных угрозах может существенно повлиять на способность финансовой организации выявлять инциденты, быстро и эффективно реагировать в случае их возникновения.

В частности, осведомленность об актуальных информационных угрозах может помочь финансовой организации проанализировать уязвимости критичной архитектуры и способствовать эффективной реализации соответствующих мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз.

Одним из важных условий достижения осведомленности финансовой организации об актуальных информационных угрозах является активный информационный обмен об инцидентах между финансовой организацией и участниками такого обмена:

- Банком России;
- федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- причастными сторонами, в том числе клиентами финансовой организации;
- иными организациями как внутри финансового сектора, так и за его пределами.

6.14 Финансовая организация классифицирует все события риска реализации информационных угроз с точки зрения следующих элементов:

- источников такого риска;
- типов событий реализации информационных угроз;
- видов (направлений) деятельности финансовой организации;
- видов потерь от реализации такого риска.

Подробное описание соответствующих классификаций событий риска реализации информационных угроз приведено в приложениях А—Г.

6.15 Выполнение процессов планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз направлено на обеспечение соответствия фактических значений КПУР принятым финансовой организацией, что достигается в том числе планированием, реализацией, контролем и совершенствованием систем управления, определенных в рамках семейств стандартов ЗИ и ОН комплекса стандартов.

Оценка зрелости процессов планирования, реализации, контроля и совершенствования систем управления, определенных в рамках семейств ЗИ и ОН комплекса стандартов, осуществляется согласно методикам оценки соответствия, определяемым в рамках соответствующего семейства стандартов комплекса стандартов, посредством внешнего аудита, с привлечением аудиторской или консалтинговой организации.

Юридические лица или индивидуальные предприниматели, привлекаемые финансовой организацией для проведения работ по обеспечению и оценке операционной надежности и защиты информации, должны иметь лицензию на осуществление деятельности по технической защите конфиденциальной информации[1)] [16].

Примечание — Финансовой организации рекомендуется для проведения внешнего аудита привлекать организации, подтвердившие соответствие своей деятельности ГОСТ Р ИСО/МЭК 27006 и ГОСТ Р ИСО/МЭК 17021-1.

6.16 В рамках осуществления деятельности финансовые организации могут выстраивать взаимодействие с иными организациями, на которых не распространяется область применения настоящего стандарта. Ввиду того, что такое взаимодействие может оказывать значительное влияние на операционную надежность финансовых организаций, крайне важно, чтобы оно базировалось на ответственном отношении к вопросам управления риском реализации информационных угроз и обеспечения операционной надежности каждой из сторон.

Примечание — Финансовой организации при выборе поставщика услуг, в том числе поставщика облачных услуг, рекомендуется привлекать организации, подтвердившие соответствие своей деятельности ГОСТ Р 57580.1.

7 Состав направлений, процессов и требований, определяемый комплексом стандартов

7.1 Финансовой организацией должны быть определены и выполняться направления, процессы, требования и меры, состав которых определяется в рамках семейств стандартов Комплекса стандартов, приведенных в разделе 5 настоящего стандарта.

[1)] В случае наличия соответствующих требований в нормативных актах Банка России [8]—[10].

7.2 Состав направлений, процессов и требований по управлению риском реализации информационных угроз и обеспечению операционной надежности, определяемый настоящим стандартом, формирующим основу семейства стандартов УР, приведен в таблице 1.

7.3 Состав направлений, процессов, требований по защите информации финансовых организаций, определяемый в рамках семейства стандартов ЗИ, приведен в таблице 2.

7.4 Состав направлений, процессов, требований по обеспечению операционной надежности, определяемый в рамках семейства стандартов ОН, приведен в таблице 3.

7.5 Состав направлений, процессов, требований и мер реализуется в рамках системы управления риском реализации информационных угроз систем управления, определенных в рамках семейств стандартов ОН и ЗИ Комплекса стандартов, с учетом структуры и взаимосвязей, приведенных на рисунке 2.

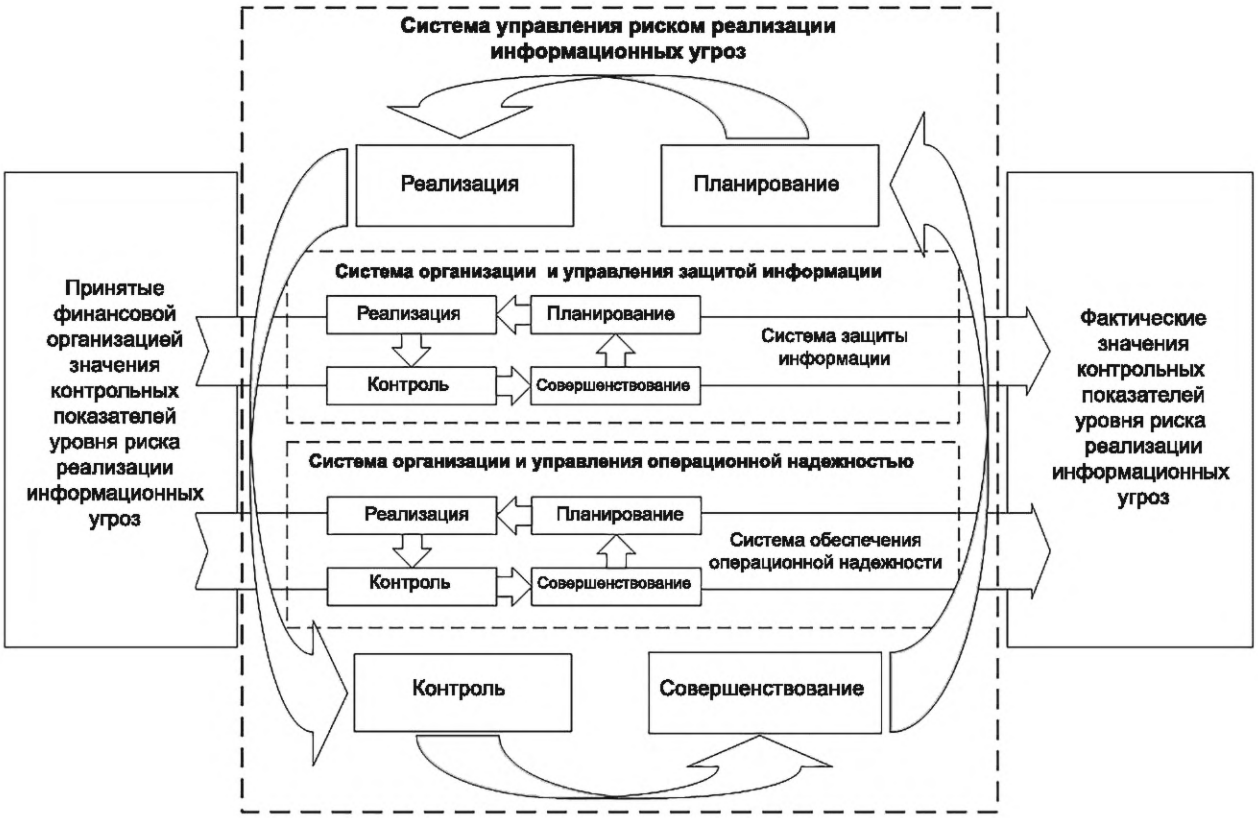

Рисунок 2 — Структура и взаимосвязи системы управления риском реализации информационных угроз финансовой организации и систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов

Таблица 1 — Состав направлений и процессов, определяемых в рамках семейства стандартов УР «Управление риском реализации информационных угроз и обеспечение операционной надежности», и требования к их реализации

Направление по управлению риском реализации информационных угроз	Процессы по управлению риском реализации информационных угроз	Подпроцессы по управлению риском реализации информационных угроз	Требования к реализации процессов
Планирование системы управления риском реализации информационных угроз	Определение политики управления риском реализации информационных угроз		Применяемые финансовой организацией меры должны обеспечивать: - установление структуры и организации системы управления риском реализации информационных угроз, а также распределение функций, ролей и ответственности в рамках управления риском реализации информационных угроз (см. таблицу 4); - установление политики управления риском реализации информационных угроз (см. таблицу 5); - участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз (см. таблицу 6)
	Выявление и идентификация риска реализации информационных угроз, а также его оценка		Применяемые финансовой организацией меры должны обеспечивать: - идентификацию критичной архитектуры (см. таблицу 1 ГОСТ Р 57580.4—2022); - идентификацию риска реализации информационных угроз (см. таблицу 7); - выявление и моделирование информационных угроз (см. таблицу 8); - оценку риска реализации информационных угроз (см. таблицу 9)
	Организация ресурсного (кадрового и финансового) обеспечения		Применяемые финансовой организацией меры должны обеспечивать: - организацию ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз (см. таблицу 10); - организацию ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ (см. таблицу 11); - организацию целевого обучения по вопросам выявления и противостояния реализации информационных угроз (см. таблицу 12)
	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	Разработка мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	Применяемые финансовой организацией меры должны обеспечивать: - выбор и применение способа реагирования на риск реализации информационных угроз (см. таблицу 13); - разработку мероприятий, направленных на снижение СВР инцидентов (см. таблицу 14); - разработку мероприятий, направленных на ограничение СТП инцидентов (см. таблицу 15)

Продолжение таблицы 1

Направление по управлению риском реализации информационных угроз	Процессы по управлению риском реализации информационных угроз	Подпроцессы по управлению риском реализации информационных угроз	Требования к реализации процессов
Реализация системы управления риском реализации информационных угроз	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	Защита от информационных угроз	Применяемые финансовой организацией меры должны обеспечивать: - защиту информации финансовой организации (см. таблицу 16); - операционную надежность (см. таблицу 17); - управление риском реализации информационных угроз при аутсорсинге (см. таблицу 18); - управление риском внутреннего нарушителя (см. таблицу 14 ГОСТ Р 57580.4—2022); - управление риском реализации информационных угроз в финансовых экосистемах (см. таблицу 19); - предотвращение утечек информации (см. таблицы 1—12, 29—31 ГОСТ Р 57580.1—2017)
	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	Реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации	Применяемые финансовой организацией меры должны обеспечивать: - реагирование на инциденты в отношении критичной архитектуры (см. таблицу 6 ГОСТ Р 57580.4—2022); - восстановление функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов (см. таблицу 7 ГОСТ Р 57580.4—2022); - проведение анализа причин и последствий реализации инцидентов (см. таблицу 8 ГОСТ Р 57580.4—2022); - организацию взаимодействия между подразделениями финансовой организации, а также между финансовой организацией и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после их реализации (см. таблицу 9 ГОСТ Р 57580.4—2022)
	Выявление событий риска реализации информационных угроз		Применяемые финансовой организацией меры должны обеспечивать: - сбор и регистрацию информации о внутренних событиях риска реализации информационных угроз и потерях (см. таблицу 20); - выявление и фиксацию инцидентов, в том числе обнаружение компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации (см. таблицу 5 ГОСТ Р 57580.4—2022); - ведение претензионной работы (см. таблицу 21)

Окончание таблицы 1

Направление по управлению риском реализации информационных угроз	Процессы по управлению риском реализации информационных угроз	Подпроцессы по управлению риском реализации информационных угроз	Требования к реализации процессов
Реализация системы управления риском реализации информационных угроз	Обеспечение осведомленности об актуальных информационных угрозах		Применяемые финансовой организацией меры должны обеспечивать: - организацию взаимодействия финансовой организации и причастных сторон, в том числе клиентов финансовой организации, при обмене информацией об актуальных сценариях реализации информационных угроз (см. таблицу 15 ГОСТ Р 57580.4—2022); - использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации (см. таблицу 16 ГОСТ Р 57580.4—2022); - повышение осведомленности работников финансовой организации в части противостояния реализации информационных угроз (см. таблицу 17 ГОСТ Р 57580.4-2022)
Контроль системы управления риском реализации информационных угроз	Установление и реализация программ контроля и аудита		Применяемые финансовой организацией меры должны обеспечивать: - проведение самооценки и профессиональной независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации (см. таблицу 22); - проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения) (см. таблицу 12 ГОСТ Р 57580.4—2022); - оценку эффективности функционирования системы управления риском реализации информационных угроз (см. таблицу 23); - организацию внутренней отчетности в рамках управления риском реализации информационных угроз (см. таблицу 24)
	Мониторинг риска реализации информационных угроз		Финансовая организация должна применять меры по мониторингу риска реализации информационных угроз (см. таблицу 25)
Совершенствование системы управления риском реализации информационных угроз	Обеспечение соответствия фактических значений КПУР принятым		Применяемые финансовой организацией меры должны обеспечивать: - проведение анализа необходимости совершенствования системы управления риском реализации информационных угроз (см. таблицу 26); - принятие решений по совершенствованию системы управления риском реализации информационных угроз (см. таблицу 27)

Таблица 2 — Состав направлений и процессов, определяемых в рамках семейства стандартов ЗИ «Защита информации финансовой организации», и требования к их реализации

Направления, процессы (подпроцессы) по защите информации		Требования к реализации направлений, процессов (подпроцессов) по защите информации
Обеспечение защиты информации при управлении доступом	Управление учетными записями и правами субъектов логического доступа	Применяемые финансовой организацией меры должны обеспечивать: - организацию и контроль использования учетных записей субъектов логического доступа (см. таблицу 1 ГОСТ Р 57580.1—2017); - организацию и контроль предоставления (отзыва) и блокирования логического доступа (см. таблицу 2 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с операциями с учетными записями и правами логического доступа, и контроль использования предоставленных прав логического доступа (см. таблицу 3 ГОСТ Р 57580.1—2017)
	Идентификация, аутентификация, авторизация (разграничение доступа) при осуществлении логического доступа	Применяемые финансовой организацией меры должны обеспечивать: - идентификацию и аутентификацию субъектов логического доступа (см. таблицу 4 ГОСТ Р 57580.1—2017); - организацию управления и организацию защиты идентификационных и аутентификационных данных (см. таблицу 5 ГОСТ Р 57580.1—2017); - авторизацию (разграничение доступа) при осуществлении логического доступа (см. таблицу 6 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с идентификацией, аутентификацией и авторизацией при осуществлении логического доступа (см. таблицу 7 ГОСТ Р 57580.1—2017)
	Защита информации при осуществлении физического доступа	Применяемые финансовой организацией меры должны обеспечивать: - организацию и контроль физического доступа в помещения, в которых расположены объекты доступа (см. таблицу 8 ГОСТ Р 57580.1—2017); - организацию и контроль физического доступа к объектам доступа, расположенным в публичных (общедоступных) местах (см. таблицу 9 ГОСТ Р 57580.1—2017); - регистрацию событий, связанных с физическим доступом (см. таблицу 10 ГОСТ Р 57580.1—2017)
	Идентификация и учет ресурсов и объектов доступа	Применяемые финансовой организацией меры должны обеспечивать: - организацию учета и контроль состава ресурсов и объектов доступа (см. таблицу 11 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с операциями по изменению состава ресурсов и объектов доступа (см. таблицу 12 ГОСТ Р 57580.1—2017)
Обеспечение защиты вычислительных сетей	Сегментация и межсетевое экранирование вычислительных сетей	Применяемые финансовой организацией меры должны обеспечивать: - сегментацию и межсетевое экранирование внутренних вычислительных сетей (см. таблицу 13 ГОСТ Р 57580.1—2017); - защиту внутренних вычислительных сетей при взаимодействии с сетью Интернет (см. таблицу 14 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с операциями по изменению параметров защиты вычислительных сетей (см. таблицу 15 ГОСТ Р 57580.1—2017)

Продолжение таблицы 2

Направления, процессы (подпроцессы) по защите информации		Требования к реализации направлений, процессов (подпроцессов) по защите информации
Обеспечение защиты вычислительных сетей	Выявление вторжений и сетевых атак	Применяемые финансовой организацией меры должны обеспечивать: - мониторинг и контроль содержимого сетевого трафика (см. таблицу 16 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с результатами мониторинга и контроля содержимого сетевого трафика (см. таблицу 17 ГОСТ Р 57580.1—2017)
	Защита информации, передаваемой по вычислительным сетям	Финансовой организацией должны применяться меры по защите информации, передаваемой по вычислительным сетям (см. таблицу 18 ГОСТ Р 57580.1—2017)
	Защита беспроводных сетей	Применяемые финансовой организацией меры должны обеспечивать: - защиту информации от раскрытия и модификации при использовании беспроводных сетей (см. таблицу 19 ГОСТ Р 57580.1—2017); - защиту внутренних вычислительных сетей при использовании беспроводных сетей (см. таблицу 20 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с использованием беспроводных сетей (см. таблицу 21 ГОСТ Р 57580.1—2017)
Контроль целостности и защищенности информационной инфраструктуры		Применяемые финансовой организацией меры должны обеспечивать: - контроль отсутствия известных (описанных) уязвимостей защиты информации объектов информатизации (см. таблицу 22 ГОСТ Р 57580.1—2017); - организацию и контроль размещения, хранения и обновления ПО информационной инфраструктуры (таблица 23 ГОСТ Р 57580.1—2017); - контроль состава и целостности ПО информационной инфраструктуры (см. таблицу 24 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с результатами контроля целостности и защищенности информационной инфраструктуры (см. таблицу 25 ГОСТ Р 57580.1—2017)
Защита от вредоносного кода		Применяемые финансовой организацией меры должны обеспечивать: - организацию эшелонированной защиты от вредоносного кода на разных уровнях информационной инфраструктуры (см. таблицу 26 ГОСТ Р 57580.1—2017); - организацию и контроль применения средств защиты от вредоносного кода (таблица 27 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с реализацией защиты от вредоносного кода (таблица 28 ГОСТ Р 57580.1—2017)

Продолжение таблицы 2

Направления, процессы (подпроцессы) по защите информации		Требования к реализации направлений, процессов (подпроцессов) по защите информации
Предотвращение утечек информации		Применяемые финансовой организацией меры должны обеспечивать: - блокирование не разрешенных к использованию и контроль разрешенных к использованию потенциальных каналов утечки информации (см. таблицу 29 ГОСТ Р 57580.1—2017); - контроль (анализ) информации, передаваемой по разрешенным к использованию потенциальным каналам утечки информации (см. таблицу 30 ГОСТ Р 57580.1—2017); - организацию защиты машинных носителей информации (см. таблицу 31 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с реализацией защиты по предотвращению утечки информации (см. таблицу 32 ГОСТ Р 57580.1—2017)
Управление инцидентами защиты информации	Мониторинг и анализ событий защиты информации	Применяемые финансовой организацией меры должны обеспечивать: - организацию мониторинга данных регистрации о событиях защиты информации, формируемых средствами и системами защиты информации, объектами информатизации, в том числе в соответствии с требованиями к содержанию базового состава мер защиты информации (см. таблицу 33 ГОСТ Р 57580.1—2017); - сбор, защиту и хранение данных регистрации о событиях защиты информации (см. таблицу 34 ГОСТ Р 57580.1—2017); - анализ данных регистрации о событиях защиты информации (см. таблицу 35 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с операциями по обработке данных регистрации о событиях защиты информации (см. таблицу 36 ГОСТ Р 57580.1—2017)
	Обнаружение инцидентов защиты информации и реагирование на них	Применяемые финансовой организацией меры должны обеспечивать: - обнаружение и регистрацию инцидентов защиты информации (см. таблицу 37 ГОСТ Р 57580.1—2017); - организацию реагирования на инциденты защиты информации (см. таблицу 38 ГОСТ Р 57580.1—2017); - организацию хранения и защиту информации об инцидентах защиты информации (см. таблицу 39 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с результатами обнаружения инцидентов защиты информации и реагирования на них (см. таблицу 40 ГОСТ Р 57580.1—2017)
Защита среды виртуализации		Применяемые финансовой организацией меры должны обеспечивать: - организацию идентификации, аутентификации, авторизации (разграничения доступа) при осуществлении логического доступа к виртуальным машинам и серверным компонентам виртуализации (см. таблицу 41 ГОСТ Р 57580.1—2017); - организацию и контроль информационного взаимодействия и изоляции виртуальных машин (см. таблицу 42 ГОСТ Р 57580.1—2017); - организацию защиты образов виртуальных машин (см. таблицу 43 ГОСТ Р 57580.1—2017); - регистрацию событий защиты информации, связанных с доступом к виртуальным машинам и серверным компонентам виртуализации (см. таблицу 44 ГОСТ Р 57580.1—2017)

Продолжение таблицы 2

Направления, процессы (подпроцессы) по защите информации	Требования к реализации направлений, процессов (подпроцессов) по защите информации
Защита информации при осуществлении удаленного логического доступа работников организации кредитно-финансовой сферы с использованием мобильных (переносных) устройств	Применяемые финансовой организацией меры должны обеспечивать: - защиту информации от раскрытия и модификации при осуществлении удаленного доступа (см. таблицу 45 ГОСТ Р 57580.1—2017); - защиту внутренних вычислительных сетей при осуществлении удаленного доступа (см. таблицу 46 ГОСТ Р 57580.1—2017); - защиту информации от раскрытия и модификации при ее обработке и хранении на мобильных (переносных) устройствах (см. таблицу 47 ГОСТ Р 57580.1—2017)
Планирование процесса системы защиты информации	В рамках направления «планирование» финансовая организация обеспечивает определение (пересмотр) (см. таблицу 48 ГОСТ Р 57580.1—2017): - области применения процесса системы защиты информации; - состава применяемых (а также неприменяемых) мер защиты информации; - состава и содержания мер защиты информации, являющихся дополнительными к базовому составу мер, определяемых на основе актуальных угроз защиты информации, требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты информации; - порядка применения мер защиты информации в рамках процесса системы защиты информации
Реализация процесса системы защиты информации	В рамках направления «реализация» финансовая организация обеспечивает (см. таблицу 49 ГОСТ Р 57580.1—2017): - должное применение мер защиты информации; - определение ролей защиты информации, связанных с применением мер защиты информации; - назначение ответственных лиц за выполнение ролей защиты информации; - доступность реализации технических мер защиты информации; - применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия [в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности], в случаях, когда применение таких средств необходимо для нейтрализации угроз безопасности, определенных в модели угроз и нарушителей безопасности информации организации кредитно-финансовой сферы; - обучение, практическую подготовку (переподготовку) работников организации кредитно-финансовой сферы, ответственных за применение мер защиты информации; - повышение осведомленности (инструктаж) работников организации кредитно-финансовой сферы в области защиты информации
Контроль процесса системы защиты информации	Применяемые финансовой организацией меры защиты информации должны обеспечивать контроль (см. таблицу 50 ГОСТ Р 57580.1—2017): - области применения процесса системы защиты информации; - должного применения мер защиты информации в рамках процесса системы защиты информации; - знаний работников организации кредитно-финансовой сферы в части применения мер защиты информации

Окончание таблицы 2

Направления, процессы (подпроцессы) по защите информации	Требования к реализации направлений, процессов (подпроцессов) по защите информации
Совершенствование процесса системы защиты информации	Применяемые финансовой организацией меры в рамках направления «совершенствование» должны обеспечивать формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотр применяемых мер защиты информации (см. таблицу 51 ГОСТ Р 57580.1—2017)
Защита информации на этапах жизненного цикла автоматизированных систем и приложений	Применяемые финансовой организацией меры на этапах жизненного цикла автоматизированных систем (далее — АС) должны обеспечивать (см. таблицы 53—56 ГОСТ Р 57580.1—2017): - определение состава мер защиты информации, реализуемых в АС (мер системы защиты информации АС); - должное применение и контроль применения мер системы защиты информации АС; - контроль отсутствия уязвимостей защиты информации в прикладном ПО АС и информационной инфраструктуре, предназначенной для размещения АС; - конфиденциальность защищаемой информации

Таблица 3 — Состав направлений и процессов, определяемых в рамках семейства стандартов ОН «Обеспечение операционной надежности», и требования к их реализации

Направления и процессы по обеспечению операционной надежности	Требования к реализации направлений и процессов по обеспечению операционной надежности
Идентификация критичной архитектуры	Применяемые финансовой организацией меры должны обеспечивать: - организацию учета и мониторинга состава элементов критичной архитектуры (см. таблицу 1 ГОСТ Р 57580.4—2022)
Управление изменениями	Применяемые финансовой организацией меры должны обеспечивать: - организацию и выполнение процедур управления изменениями в критичной архитектуре (см. таблицу 2 ГОСТ Р 57580.4—2022), направленных на: предотвращение возникновения уязвимостей в критичной архитектуре, с использованием которых могут реализовываться информационные угрозы и которые могут повлечь превышение (отклонение от) значений целевых показателей операционной надежности; планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение (повышение) операционной надежности финансовой организации; - управление конфигурациями объектов информатизации, входящих в критичную архитектуру (см. таблицу 3 ГОСТ Р 57580.4—2022); - управление уязвимостями и обновлениями (исправлениями) объектов информатизации, входящих в критичную архитектуру (см. таблицу 4 ГОСТ Р 57580.4—2022)

Продолжение таблицы 3

Направления и процессы по обеспечению операционной надежности	Требования к реализации направлений и процессов по обеспечению операционной надежности
Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации	Применяемые финансовой организацией меры должны обеспечивать: - выявление и фиксацию инцидентов, в том числе обнаружение компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации (см. таблицу 5 ГОСТ Р 57580.4—2022); - реагирование на инциденты в отношении критичной архитектуры (см. таблицу 6 ГОСТ Р 57580.4—2022); - восстановление функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов (см. таблицу 7 ГОСТ Р 57580.4—2022); - проведение анализа причин и последствий реализации инцидентов (см. таблицу 8 ГОСТ Р 57580.4—2022); - организацию взаимодействия между подразделениями финансовой организации, а также между финансовой организацией и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после их реализации (см. таблицу 9 ГОСТ Р 57580.4—2022)
Взаимодействие с поставщиками услуг	Применяемые финансовой организацией меры должны обеспечивать: - управление риском реализации информационных угроз при привлечении поставщиков услуг, в том числе защиту объектов информатизации, входящих в критичную архитектуру, от возможной реализации информационных угроз, включая компьютерные атаки, со стороны поставщиков услуг (см. таблицу 10 ГОСТ Р 57580.4—2022); - управление риском технологической зависимости функционирования объектов информатизации финансовой организации от поставщиков услуг (см. таблицу 11 ГОСТ Р 57580.4—2022)
Тестирование операционной надежности бизнес- и технологических процессов	Финансовая организация должна применять меры по проведению сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения) (см. таблицу 12 ГОСТ Р 57580.4—2022)
Защита критичной архитектуры от возможной реализации информационных угроз при организации удаленной работы	Финансовая организация должна применять меры по защите критичной архитектуры от возможной реализации информационных угроз при организации удаленной работы (см. таблицу 13 ГОСТ Р 57580.4—2022)
Управление риском внутреннего нарушителя	Финансовая организация должна применять меры по управлению риском внутреннего нарушителя (см. таблицу 14 ГОСТ Р 57580.4—2022)
Обеспечение осведомленности об актуальных информационных угрозах	Применяемые финансовой организацией меры должны обеспечивать: - организацию взаимодействия финансовой организации и причастных сторон, в том числе клиентов финансовой организации, при обмене информацией об актуальных сценариях реализации информационных угроз (см. таблицу 15 ГОСТ Р 57580.4—2022); - использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации (см. таблицу 16 ГОСТ Р 57580.4—2022); - повышение осведомленности работников финансовой организации в части противостояния реализации информационных угроз (см. таблицу 17 ГОСТ Р 57580.4—2022

Окончание таблицы 3

Направления и процессы по обеспечению операционной надежности	Требования к реализации направлений и процессов по обеспечению операционной надежности
Планирование процесса системы обеспечения операционной надежности	В рамках направления «планирование» финансовая организация обеспечивает определение (пересмотр) (см. таблицу 18 ГОСТ Р 57580.4—2022): - области применения процесса обеспечения операционной надежности; - состава применяемых (а также неприменяемых) мер обеспечения операционной надежности; - состава и содержания мер обеспечения операционной надежности, являющихся дополнительными к базовому составу мер, определяемых на основе актуальных информационных угроз; - порядка применения мер обеспечения операционной надежности в рамках процесса обеспечения операционной надежности
Реализация процесса системы обеспечения операционной надежности	В рамках направления «реализация» финансовая организация обеспечивает (см. таблицу 19 ГОСТ Р 57580.4—2022): - должное применение организационных и технических мер; - назначение ответственных лиц за выполнение ролей по обеспечению операционной надежности; - доступность реализации технических мер; - обучение, практическую подготовку (переподготовку) работников финансовой организации, ответственных за применение организационных и технических мер; - повышение осведомленности (инструктаж) работников финансовой организации в области обеспечения операционной надежности
Контроль процесса системы обеспечения операционной надежности	Применяемые финансовой организацией меры должны обеспечивать контроль (см. таблицу 20 ГОСТ Р 57580.4—2022): - области применения процесса обеспечения операционной надежности; - должного применения организационных и технических мер; - знаний работников финансовой организации в части применения организационных и технических мер
Совершенствование процесса системы обеспечения операционной надежности	Применяемые финансовой организацией меры в рамках направления «совершенствование» должны обеспечивать формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотр применяемых мер обеспечения операционной надежности (см. таблицу 21 ГОСТ Р 57580.4—2022)

8 Требования к системе управления риском реализации информационных угроз

8.1 Общие положения

8.1.1 Настоящий раздел устанавливает требования к мерам по управлению риском реализации информационных угроз для следующих направлений:

а) направление 1 «планирование системы управления риском реализации информационных угроз» (см. таблицы 4—12);

б) направление 2 «реализация системы управления риском реализации информационных угроз» (см. таблицы 13—21);

в) направление 3 «контроль системы управления риском реализации информационных угроз» (см. таблицы 22—25);

г) направление 4 «совершенствование системы управления риском реализации информационных угроз» (см. таблицы 26, 27).

8.1.2 Способы реализации мер по управлению риском реализации информационных угроз, установленные в таблицах раздела 8 настоящего стандарта, обозначены следующим образом:

- «О» — реализация путем применения организационной меры[1)];
- «Т» — реализация путем применения технической меры;
- «Н» — реализация является необязательной.

8.2 Направление 1 «Планирование системы управления риском реализации информационных угроз»

8.2.1 Процесс «Определение политики управления риском реализации информационных угроз»

8.2.1.1 Применяемые финансовой организацией меры по определению политики управления риском реализации информационных угроз должны обеспечивать:

- установление структуры и организации системы управления риском реализации информационных угроз, а также распределение функций, ролей и ответственности в рамках управления риском реализации информационных угроз;
- установление политики управления риском реализации информационных угроз;
- участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз.

При реализации процесса «Определение политики управления риском реализации информационных угроз» рекомендуется использовать ГОСТ Р ИСО/МЭК 27001, а также [17].

8.2.1.2 Состав мер по установлению структуры и организации системы управления риском реализации информационных угроз, а также распределению функций, ролей и ответственности в рамках управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 4.

[1)] По решению финансовой организации способ «О» может быть реализован путем применения технической меры.

Таблица 4 — Состав мер по установлению структуры и организации системы управления риском реализации информационных угроз, а также распределению функций, ролей и ответственности в рамках управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.1	Установление во внутренних документах финансовой организации структуры и организации системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ, включая:	—	—	—
ОПР.1.1	- определение и описание состава процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.1.2	- описание структуры и подходов к интеграции процессов управления риском реализации информационных угроз в систему управления операционным риском финансовой организации	О	О	О
ОПР.1.3	- определение организационной структуры финансовой организации, задействованной в выполнении процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, в том числе установление функций подразделений финансовой организации (включая принятие решений с учетом исключения конфликта интересов) и контроль за выполнением процессов в рамках порядка организации и осуществления финансовой организацией внутреннего контроля	О	О	О
ОПР.1.4	- выделение ресурсного (кадрового и финансового) обеспечения для выполнения процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.1.5	- порядок утверждения и условия пересмотра структуры и организации систем управления риском реализации информационных угроз, операционной надежности и защиты информации	О	О	О
ОПР.2	Реализация механизмов взаимодействия и координации деятельности* вовлеченных подразделений, формирующих «три линии защиты», а также причастных сторон (за исключением клиентов финансовой организации) в целях подготовки и реализации политики управления риском реализации информационных угроз	О	О	О
ОПР.3	Определение должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз** финансовой организации (в том числе согласно требованиям нормативных актов Банка России [3]): - имеющего прямое подчинение лицу, осуществляющему функции единоличного исполнительного органа финансовой организации; - не участвующего в совершении операций, сделок, организации бухгалтерского и управленческого учета, обеспечении функционирования объектов информатизации; - обладающего достаточными знаниями, компетенцией, полномочиями и ресурсами (кадровыми и финансовыми) для принятия руководящих решений по вопросам управления риском реализации информационных угроз; - имеющего возможность прямого информирования единоличного исполнительного органа финансовой организации по вопросам, связанным с управлением риском реализации информационных угроз	О	О	О

Продолжение таблицы 4

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.4	Установление функций и полномочий подразделений, формирующих «первую линию защиты», включающих: - идентификацию риска реализации информационных угроз (в пределах своей компетенции) в рамках реализуемых ими бизнес- и технологических процессов; - сбор информации и информирование о внутренних событиях риска реализации информационных угроз и потерях подразделения, ответственного за регистрацию такой информации в базе событий риска реализации информационных угроз (службы ИБ); - участие в оценке риска реализации информационных угроз (в пределах компетенции) в рамках реализуемых ими бизнес- и технологических процессов; - обеспечение соблюдения требований к планированию, реализации, контролю (в пределах компетенции) и совершенствованию мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	О	О	О
ОПР.5	Установление функций и полномочий службы ИБ***:	—	—	—
ОПР.5.1	В целях обеспечения ИБ: - разработка и (или) пересмотр внутренних документов в области обеспечения операционной надежности и защиты информации; - планирование, реализация (в том числе установление требований) и контроль процессов обеспечения операционной надежности и защиты информации; - разработка предложений по совершенствованию процессов обеспечения операционной надежности и защиты информации (по результатам анализа необходимости совершенствования систем управления, определяемых в рамках семейств стандартов ОН и ЗИ); - выявление и фиксация инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации; - формирование отчетности по вопросам обеспечения операционной надежности и защиты информации, направляемой на рассмотрение коллегиальному исполнительному органу, должностному лицу, ответственному за функционирование системы управления риском реализации информационных угроз, а также иным должностным лицам, в случае наличия соответствующих требований во внутренних документах финансовой организации или требований нормативных актов Банка России [6]; осуществление других функций, связанных с реализаций процессов обеспечения операционной надежности и защиты информации, предусмотренных внутренними документами финансовой организации	О	О	О
ОПР.5.2	В целях управления риском реализации информационных угроз: - разработка и (или) пересмотр внутренних документов во взаимодействии с иными подразделениями, формирующими «вторую линию защиты» в области управления риском реализации информационных угроз, в том числе политики управления риском реализации информационных угроз и документов, определяющих методологию в рамках управления таким риском; - идентификация риска реализации информационных угроз (в том числе во взаимодействии с подразделениями, формирующими «первую линию защиты»); - сбор и регистрация информации о событиях риска реализации информационных угроз и потерях в базе событий такого риска (в том числе во взаимодействии с подразделениями, формирующими «первую линию защиты»);	О	О	О

Продолжение таблицы 4

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.5.2	- ведение базы событий риска реализации информационных угроз; - мониторинг риска реализации информационных угроз (в том числе во взаимодействии с подразделениями, формирующими «первую линию защиты»), включая определение и мониторинг значений КИР в целях контроля за возможным превышением сигнальных и контрольных значений КПУР; - планирование, реализация (в том числе установление требований) и контроль во взаимодействии с иными подразделениями, формирующими «вторую линию защиты», мероприятий, направленных на уменьшение негативного влияния от риска реализации информационных угроз*4; - разработка предложений по совершенствованию процессов управления риском реализации информационных угроз (по результатам анализа необходимости совершенствования систем управления риском реализации информационных угроз); - расчет и обоснование сигнальных и контрольных значений КПУР, характеризующих уровень зрелости процессов обеспечения операционной надежности и защиты информации, а также уровень обеспечения операционной надежности бизнес- и технологических процессов финансовой организации; - расчет фактических значений КПУР, характеризующих уровень зрелости процессов обеспечения операционной надежности и защиты информации, а также уровень обеспечения операционной надежности бизнес- и технологических процессов финансовой организации; - осуществление мониторинга риска реализации информационных угроз, включая мониторинг соблюдения сигнальных и контрольных значений КПУР; - организация процесса обеспечения осведомленности об актуальных информационных угрозах; - разработка предложений по ресурсному (кадровому и финансовому) обеспечению службы ИБ; - участие в реализации программ контроля и аудита операционной надежности и защиты информации (в части самооценки и независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации); - разработка предложений по совершенствованию системы управления риском реализации информационных угроз; - формирование отчетности в рамках управления риском реализации информационных угроз, направляемой на рассмотрение коллегиальному исполнительному органу, должностному лицу, ответственному за функционирование системы управления риском реализации информационных угроз, а также иным должностным лицам, в случае наличия соответствующих требований во внутренних документах финансовой организации или требований нормативных актов Банка России [6]; - информирование работников финансовой организации по вопросам, связанным с управлением риском реализации информационных угроз; - осуществление других функций, связанных с управлением риском реализации информационных угроз, предусмотренных внутренними документами финансовой организации	О	О	О
ОПР.6	Установление функций и полномочий подразделений, формирующих «вторую линию защиты» в части управления риском реализации информационных угроз, включающих: - интеграцию системы управления риском реализации информационных угроз в систему управления операционным риском; - координацию деятельности по управлению риском реализации информационных угроз как одним из видов операционного риска; - валидацию КИР;	О	О	О

Продолжение таблицы 4

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.6	- расчет и обоснование сигнальных и контрольных значений КПУР (за исключением сигнальных и контрольных значений КПУР, расчет и обоснование которых осуществляется службой ИБ согласно ОПР.5.2 настоящей таблицы); - расчет фактических значений КПУР (за исключением фактических значений КПУР, расчет которых осуществляется службой ИБ согласно ОПР.5.2 настоящей таблицы); - координацию деятельности по отражению информации о событиях риска реализации информационных угроз в базе событий операционного риска; - включение отчетности, формируемой в рамках управления риском реализации информационных угроз, в отчетность об управлении операционным риском; - определение (во взаимодействии со службой ИБ) согласованной или единой методологии управления риском реализации информационных угроз, обеспечивающей интеграцию процессов управления риском реализации информационных угроз в рамках процессов управления операционным риском	О	О	О
ОПР.7	Установление функций и полномочий подразделений, формирующих «третью линию защиты», в части управления риском реализации информационных угроз, включающих проведение ежегодной оценки эффективности функционирования системы управления риском реализации информационных угроз*[5], в том числе в целях: - валидации и верификации методологии и данных об управлении риском реализации информационных угроз (оценка адекватности методологии на предмет ее согласованности с внутренними политиками и требованиями финансовой организации, проверка полноты и корректности данных о риске реализации информационных угроз и событиях такого риска); - валидации внутренней отчетности в рамках управления риском реализации информационных угроз, представляемой на рассмотрение совету директоров (наблюдательному совету); - содействия своевременному и адекватному реагированию подразделениями, формирующими «первую» и «вторую линии защиты», на недостатки функционирования системы управления риском реализации информационных угроз (в части их устранения); - оценки соблюдения требований нормативных актов Банка России, в частности, [6]	О	О	О

* Реализация механизмов взаимодействия и координации деятельности может быть реализована, например, посредством постоянно действующего комитета по вопросам управления риском реализации информационных угроз. К функциям указанного комитета рекомендуется относить:

- рассмотрение вопросов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации с учетом требований (стратегии, потребностей, видения) и целей вовлеченных подразделений, формирующих «три линии защиты», и причастных сторон (за исключением клиентов финансовой организации), ресурсного (кадрового и финансового) обеспечения и применяемых объектов информатизации;

- разработку состава КПУР, а также их сигнальных и контрольных значений с учетом требований (стратегий, потребностей, видения) вовлеченных подразделений, формирующих «три линии защиты»;

- распределение и согласование задач, координацию взаимодействия вовлеченных подразделений, формирующих «три линии защиты», и причастных сторон (за исключением клиентов финансовой организации) в рамках процессов планирования, реализации, контроля и совершенствования системы управления риском информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов;

Окончание таблицы 4

- обеспечение данных для мониторинга деятельности вовлеченных подразделений, формирующих «три линии защиты», и причастных сторон (за исключением клиентов финансовой организации) по выполнению процессов планирования, реализации, контроля и совершенствования системы управления риском информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов.

Функции комитета по вопросам управления риском реализации информационных угроз могут быть реализованы в рамках иного комитета, например комитета по управлению рисками.

** При принятии финансовой организацией решения о создании отдельных систем управления под каждый вид риска реализации информационных угроз (согласно примечанию к 3.8) для каждой системы управления может быть назначено отдельное ответственное должностное лицо, с соблюдением предъявляемых в рамках ОПР.3 требований к такому лицу.

*** Рекомендуется относить функции и полномочия службы ИБ ко «второй линии защиты». Допускается отнесение отдельных функций и полномочий, перечисленных в ОПР.5.1 и ОПР.5.2 настоящей таблицы, к функциям и полномочиям иных подразделений, если иное не установлено нормативными актами Банка России [6]. В случае принятия финансовой организацией отдельных функций и полномочий службы ИБ к функциям и полномочиям иных подразделений положения настоящего стандарта также применяются в отношении соответствующих подразделений.

*4 За исключением планирования, реализации, контроля и совершенствования процессов обеспечения операционной надежности и защиты информации.

*5 В составе оценки эффективности функционирования системы управления операционным риском.

8.2.1.3 Состав мер по установлению политики управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 5.

Таблица 5 — Состав мер по установлению политики управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.8	Установление политикой управления риском реализации информационных угроз основных принципов функционирования системы управления таким риском:	—	—	—
ОПР.8.1	- направленность на обеспечение операционной надежности финансовой организации	О	О	О
ОПР.8.2	- интеграция системы управления риском реализации информационных угроз в систему управления операционным риском финансовой организации	О	О	О
ОПР.8.3	- соответствие политики управления риском реализации информационных угроз, а также устанавливаемых ею приоритетов общим бизнес-целям финансовой организации	О	О	О
ОПР.8.4	- систематический и проактивный подход в части противостояния возможным информационным угрозам	О	О	О
ОПР.8.5	- участие совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.9	Установление политикой управления риском реализации информационных угроз следующих задач управления таким риском:	—	—	—
ОПР.9.1	- обеспечение возможности покрытия потерь финансовой организации, причастных сторон, в том числе клиентов финансовой организации, в результате инцидентов, в том числе за счет формирования финансового резерва и (или) страхования риска реализации информационных угроз*	О	О	О

Продолжение таблицы 5

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.9.2	- обеспечение возможности поддержания непрерывного предоставления финансовых и (или) информационных услуг в условиях возможной реализации информационных угроз	О	О	О
ОПР.9.3	- защиты интересов клиентов финансовой организации в случае их потерь в результате инцидентов	О	О	О
ОПР.9.4	- соблюдения требований законодательства Российской Федерации в области защиты информации, устанавливаемых на основании статей 57.4 и 76.4-1 Федерального закона [1], части 3 статьи 27 Федерального закона [11], а также устанавливаемых статьей 19 Федерального закона [12], статьей 16 Федерального закона [13] и Федеральным законом [14]	О	О	О
ОПР.10	Установление целей и требований политики управления риском реализации информационных угроз с участием и по согласованию с вовлеченными подразделениями, формирующими «три линии защиты»	О	О	О
ОПР.11	Установление политикой управления риском реализации информационных угроз в целях контроля за достижением целей управления таким риском состава КПУР**, а также их сигнальных и контрольных значений по следующим группам:	—	—	—
ОПР.11.1	- группа КПУР, характеризующих уровень совокупных потерь финансовой организации в результате событий риска реализации информационных угроз	О	О	О
ОПР.11.2	- группа КПУР, характеризующих уровень операционной надежности бизнес- и технологических процессов финансовой организации	О	О	О
ОПР.11.3	группа КПУР, характеризующих уровень несанкционированных операций (потерь клиентов финансовой организации) в результате инцидентов	О	О	О
ОПР.12	Установление политикой управления риском реализации информационных угроз допустимого уровня такого риска (риск-аппетита финансовой организации) с учетом сигнальных и контрольных значений КПУР**	О	О	О
ОПР.13	Установление политикой управления риском реализации информационных угроз основных принципов и подходов к организации контроля за функционированием системы управления таким риском, включая:	—	—	—
ОПР.13.1	- пересмотр (в том числе условия пересмотра) политики управления риском реализации информационных угроз при изменении целей финансовой организации, в том числе в части допустимого уровня такого риска (риск-аппетита финансовой организации), существенных изменений в критичной архитектуре, существенного изменения модели информационных угроз	О	О	О
ОПР.13.2	- организацию внутренней отчетности в рамках управления риском реализации информационных угроз, включая внутреннюю отчетность об уровне зрелости процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.13.3	- валидацию и верификацию со стороны подразделений, формирующих «третью линии защиты», методологии, данных и внутренней отчетности в рамках управления риском реализации информационных угроз	О	О	О
ОПР.13.4	- адекватное и своевременное реагирование на неудовлетворительные результаты валидации и верификации	О	О	О

Окончание таблицы 5

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.14	Установление политикой управления риском реализации информационных угроз требований к созданию ресурсных (кадровых и финансовых) условий для обеспечения необходимого уровня зрелости процессов управления таким риском, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.15	Установление политикой управления риском реализации информационных угроз требований к привлекаемым в рамках аутсорсинга бизнес- и технологических процессов, а также процессов обеспечения операционной надежности и защиты информации поставщикам услуг, в том числе поставщикам облачных услуг (в части установления требуемого уровня зрелости процессов обеспечения операционной надежности и защиты информации в рамках соглашения об аутсорсинге), а также порядка взаимодействия и распределения ответственности между финансовой организацией и поставщиками услуг, в том числе поставщиками облачных услуг	О	О	О
ОПР.16	Установление политикой управления риском реализации информационных угроз функций и ответственности коллегиального исполнительного органа и работников финансовой организации в рамках управления риском реализации информационных угроз	О	О	О
ОПР.17	Установление политикой управления риском реализации информационных угроз области применения системы управления таким риском	О	О	О
* В случае если требованиями нормативных актов Банка России не предусмотрено формирование резервов на покрытие потерь от реализации операционного риска, финансовые организации самостоятельно определяют способы покрытия потерь в результате инцидентов. ** Состав КПУР по каждой группе, а также их сигнальные и контрольные значения приведены в приложениях Д, Е.				

8.2.1.4 Состав мер по участию совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации применительно к уровням защиты приведен в таблице 6.

Примечание — Состав мер, приведенных в таблице 6, применяется в части, не противоречащей законодательству Российской Федерации [18], [19], а также требованиям нормативных актов Банка России [6].

Таблица 6 — Состав мер по участию совета директоров (наблюдательного совета) и коллегиального исполнительного органа финансовой организации в решении вопросов управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.18	Установление внутренними документами финансовой организации распределения зон компетенции* совета директоров (наблюдательного совета), коллегиального исполнительного органа финансовой организации (а в случае его отсутствия — единоличного исполнительного органа) и подотчетных им коллегиальных органов в части решения вопросов, связанных с управлением риском реализации информационных угроз, обеспечением операционной надежности и защиты информации	Н	О	О

Продолжение таблицы 6

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.19	Отнесение к зоне компетенции совета директоров (наблюдательного совета), коллегиального исполнительного органа финансовой организации (а в случае его отсутствия — единоличного исполнительного органа) или подотчетных им коллегиальных органов финансовой организации следующих вопросов**, связанных с управлением риском реализации информационных угроз:	—	—	—
ОПР.19.1	- утверждение политики управления риском реализации информационных угроз***	О	О	О
ОПР.19.2	- рассмотрение вопросов, связанных с управлением риском реализации информационных угроз, при возможном влиянии такого риска на принимаемые решения, связанные с общей стратегией развития финансовой организации*[4]	О	О	О
ОПР.19.3	- утверждение допустимого уровня риска реализации информационных угроз (риск-аппетита финансовой организации), состава КПУР, а также их сигнальных и контрольных значений	О	О	О
ОПР.19.4	- обеспечение как минимум ежегодного контроля за реализацией политики управления риском реализации информационных угроз и соблюдения установленных значений КПУР	О	О	О
ОПР.19.5	- обеспечение как минимум ежегодного контроля за деятельностью в части планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов	О	О	О
ОПР.19.6	- рассмотрение отчета об управлении риском реализации информационных угроз (в составе отчета об управлении операционным риском) за год	О	О	О
ОПР.19.7	- рассмотрение отчета о результатах оценки эффективности функционирования системы управления риском реализации информационных угроз (в составе отчета о результатах оценки эффективности системы управления операционным риском)	О	О	О
ОПР.19.8	- рассмотрение вопросов планирования и достаточности ресурсного (кадрового и финансового) - обеспечения для реализации политики управления риском реализации информационных угроз, а также поддержания функционирования структуры и организации систем управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
ОПР.19.9	- обеспечение реагирования финансовой организации в случае превышения сигнальных и контрольных значений КПУР	О	О	О
ОПР.19.10	- ответственность за соблюдение требований политики управления риском реализации информационных угроз	О	О	О
ОПР.19.11	- организация деятельности в целях реализации политики управления риском реализации информационных угроз	О	О	О
ОПР.19.12	- утверждение структуры и организации системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, и контроль за поддержанием функционирования таких систем	О	О	О

Окончание таблицы 6

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОПР.19.13	- организация и контроль за деятельностью по представлению на рассмотрение необходимой отчетности для контроля за реализацией политики управления риском реализации информационных угроз и соблюдения установленных значений КПУР	О	О	О
ОПР.19.14	- периодический контроль за фактическими значениями КПУР	О	О	О
ОПР.19.15	- контроль за осуществлением мониторинга риска реализации информационных угроз	Н	Н	О
ОПР.19.16	- управление ресурсным (кадровым и финансовым) обеспечением для целей в рамках выполнения процессов системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов	О	О	О
ОПР.20	Отнесение к зоне компетенции совета директоров (наблюдательного совета) или коллегиального исполнительного органа (а в случае его отсутствия — единоличного исполнительного органа) финансовой организации вопросов, связанных с формированием корпоративной этики (культуры), предполагающей:	—	—	—
ОПР.20.1	- признание и закрепление важной роли и высокой ответственности каждого работника финансовой организации в части управления риском реализации информационных угроз, включая противостояние реализации информационных угроз	О	О	О
ОПР.20.2	- организация определения способов мотивации работников финансовой организации по участию в управлении риском реализации информационных угроз, а также осведомленности об актуальных информационных угрозах в целях противостояния реализации информационных угроз	О	О	О

* В том числе на случай кризисных (чрезвычайных или нештатных) ситуаций, требующих выполнения мероприятий по обеспечению непрерывности и восстановлению деятельности финансовой организации.

** В случае если иное не установлено нормативными актами Банка России [6].

*** Финансовая организация может определять политику управления риском реализации информационных угроз как отдельный документ, так и включать в состав иных внутренних документов, определяющих правила управления рисками или обеспечения информационной безопасности в финансовой организации. Утверждение включает рассмотрение политики управления риском реализации информационных угроз, а также устанавливаемых ею приоритетов на предмет согласованности с общими бизнес-целями финансовой организации, с учетом мнения подразделений, формирующих «три линии защиты».

*[4] При принятии решений, связанных с общей стратегией развития финансовой организации, целесообразно принимать во внимание влияние принимаемых решений на уровень риска реализации информационных угроз, а также операционную надежность финансовой организации (в частности, влияние на предоставление финансовых и (или) информационных услуг).

8.2.2 Процесс «Выявление и идентификация риска реализации информационных угроз, а также его оценка»

8.2.2.1 Применяемые финансовой организацией меры по оценке риска реализации информационных угроз должны обеспечивать:

- идентификацию критичной архитектуры[1)];
- идентификацию риска реализации информационных угроз;
- выявление и моделирование информационных угроз;
- оценку риска реализации информационных угроз.

[1)] Как области применения системы управления риском реализации информационных угроз.

При реализации процесса «Выявление и идентификация риска реализации информационных угроз, а также его оценка» рекомендуется использовать ГОСТ Р ИСО 31000, ГОСТ Р 58771, ГОСТ Р ИСО/МЭК 27005, а также [20].

8.2.2.2 Состав мер по идентификации критичной архитектуры применительно к уровням защиты приведен в рамках семейства ОН комплекса стандартов.

8.2.2.3 Состав мер по идентификации риска реализации информационных угроз применительно к уровням защиты приведен в таблице 7.

Таблица 7 — Состав мер по идентификации риска реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.1	Организация* и выполнение деятельности по анализу базы событий риска реализации информационных угроз	О	О	О
ВИО.2	Организация и выполнение деятельности по проведению периодической (как минимум ежегодной) самооценки риска реализации информационных угроз	Н	Н	О
ВИО.3	Организация и выполнение деятельности по интервьюированию работников финансовой организации, в том числе с целью оценки внутренних и внешних условий и факторов, создающих условия для возникновения риска реализации информационных угроз**	Н	Н	Н
ВИО.4	Организация и выполнение деятельности по анализу актов проверок, судебных актов (решений, определений, постановлений) и (или) актов исполнительных органов государственной власти, Банка России в части фактов, относящихся к реализации риска реализации информационных угроз	Н	Н	Н
ВИО.5	Организация и выполнение деятельности по анализу информации, полученной от подразделений, формирующих «третью линию защиты», и (или) в рамках внешнего аудита	Н	Н	Н
ВИО.6	Организация и выполнение деятельности по анализу информации, полученной в рамках инициативного информирования работниками финансовой организации подразделений, формирующих «вторую линию защиты» и «третью линию защиты»	Н	Н	Н
ВИО.7	Организация и выполнение деятельности по анализу иных внешних и внутренних источников информации, способствующей выявлению риска реализации информационных угроз***	Н	Н	Н

* Под «организацией деятельности» понимается отражение во внутренних документах финансовой организации ведения соответствующей деятельности и распределение ролей по ее выполнению.

** В случае наличия (выявления) такой необходимости.

*** Например, мониторинг внешних информационных ресурсов, участие в мероприятиях по обмену опытом, в том числе сотрудничество с Банком России и соответствующими исполнительными органами государственной власти на предмет обмена опытом об эффективных практиках в части управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации.

8.2.2.4 Состав мер по выявлению и моделированию информационных угроз применительно к уровням защиты приведен в таблице 8.

Таблица 8 — Состав мер по выявлению и моделированию информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.8	Организация и выполнение на регулярной основе деятельности по определению и анализу возможных информационных угроз: - присущих осуществлению видов деятельности финансовой организации; - присущих взаимодействию финансовой организации с причастными сторонами	О	О	О
ВИО.9	Организация и выполнение на регулярной основе деятельности по определению и анализу возможных информационных угроз путем:	—	—	—
ВИО.9.1	- выявления возможных источников информационных угроз	О	О	О
ВИО.9.2	- оценки возможностей нарушителя безопасности информации	О	О	О
ВИО.9.3	- выявления возможных уязвимостей критичной архитектуры	О	О	О
ВИО.9.4	- определения возможных сценариев реализации информационных угроз	Н	О	О
ВИО.10	Организация и выполнение деятельности по выявлению возможных источников информационных угроз, присущих осуществлению видов деятельности финансовой организации, в отношении элементов идентифицированной критичной архитектуры:	—	—	—
ВИО.10.1	- бизнес- и технологических процессов	О	О	О
ВИО.10.2	- объектов информатизации	О	О	О
ВИО.10.3	- субъектов доступа	О	О	О
ВИО.10.4	- информационных потоков защищаемой информации*, обрабатываемой и передаваемой в рамках бизнес- и технологических процессов	Н	О	О
ВИО.11	Организация и выполнение деятельности по выявлению возможных источников информационных угроз, присущих взаимодействию финансовой организации с причастными сторонами, в отношении элементов идентифицированной критичной архитектуры:	—	—	—
ВИО.11.1	- бизнес- и технологических процессов, переданных на аутсорсинг и (или) выполняемых с применением сторонних информационных сервисов	О	О	О
ВИО.11.2	- взаимосвязей и взаимозависимостей между финансовой организацией и причастными сторонами (за исключением клиентов финансовой организации) в рамках выполнения бизнес- и технологических процессов, в том числе взаимосвязей и взаимозависимостей объектов информатизации	Н	О	О
ВИО.11.3	- сторонних информационных сервисов поставщиков услуг	Н	О	О
ВИО.12	Организация и выполнение деятельности по оценке возможностей нарушителя безопасности информации в отношении:	О	О	О
ВИО.12	- внутреннего нарушителя безопасности информации; - внешнего нарушителя безопасности информации	—	—	—
ВИО.13	Организация и выполнение деятельности по выявлению возможных уязвимостей критичной архитектуры путем выполнения мер, приведенных в таблице 4 ГОСТ Р 57580.4-202_	О	О	О

Окончание таблицы 8

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.14	Организация и выполнение деятельности по определению возможных сценариев реализации информационных угроз путем анализа существующих техник, тактик и процедур реализации информационных угроз на основе: - накопленного финансовой организацией опыта, в том числе в рамках реагирования на инциденты и восстановления после их реализации; - результатов проведения сценарного анализа и тестирования готовности финансовой организации противостоять реализации информационных угроз; - сценариев, разрабатываемых и распространяемых доверенными причастными сторонами; - сценариев, разрабатываемых и распространяемых Банком России	Н	О	О
ВИО.15	Разработка модели информационных угроз на основе результатов, полученных при реализации мер ВИО.8 — ВИО.14 настоящей таблицы	О	О	О
ВИО.16	Организация и выполнение деятельности по пересмотру модели информационных угроз на регулярной основе или в случаях: - выявления информации, свидетельствующей о появлении новых информационных угроз, присущих осуществлению видов деятельности финансовой организации и (или) взаимодействию финансовой организации с причастными сторонами; - выявления событий риска реализации информационных угроз в результате реализации новых информационных угроз	О	О	О
* К защищаемой информации относится информация, перечень которой определен в [8]—[10].				

8.2.2.5 Состав мер по оценке риска реализации информационных угроз применительно к уровням защиты приведен в таблице 9.

Таблица 9 — Состав мер по оценке риска реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.17	Определение и применение методологии оценки риска реализации информационных угроз, включающей:	—	—	—
ВИО.17.1	- оценку СВР событий риска*	О	О	О
ВИО.17.2	- оценку СТП событий риска*	О	О	О
ВИО.17.3	- агрегированную оценку уровня риска реализации информационных угроз** с точки зрения элементов классификации такого риска (приведенных в приложениях А — Г), в том числе в соответствии с требованиями нормативных актов Банка России [6]	О	О	О
ВИО.17.4	- оценку объема капитала, выделяемого финансовой организацией на покрытие запланированных и незапланированных потерь от реализации риска реализации информационных угроз**, в том числе в соответствии с требованиями нормативных актов Банка России [6]	Н	О	О
ВИО.18	Оценка СВР инцидентов для каждого бизнес- и технологического процесса с учетом:	—	—	—
ВИО.18.1	- результатов выявления и моделирования информационных угроз	О	О	О

Продолжение таблицы 9

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.18.2	- оценки зрелости процессов применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов [8] — [10], [21]	Н	О	О
ВИО.18.3	- оценки зрелости процессов реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня [8] — [10]	Н	О	О
ВИО.18.4	- оценки зрелости процессов планирования, реализации, контроля и совершенствования системы управления, определенной в рамках семейства стандартов ЗИ комплекса стандартов	О	О	О
ВИО.18.5	- оценки зрелости процессов планирования, реализации, контроля и совершенствования системы управления, определенной в рамках семейства стандартов ОН Комплекса стандартов	О	О	О
ВИО.19	Оценка СТП инцидентов для каждого бизнес- и технологического процесса с учетом:	—	—	—
ВИО.19.1	- уровня критичности (определяемого финансовой организацией самостоятельно, если иное не установлено нормативными актами Банка России [6]) соответствующего бизнес- и технологического процесса в рамках осуществления финансовой организацией вида деятельности, связанного с предоставлением финансовых и (или) информационных услуг	О	О	О
ВИО.19.2	- оценки соблюдения в случае реализации инцидентов значений КПУР, установленных политикой управления риском информационных угроз, в части: способности финансовой организации обеспечить покрытие финансовых потерь в результате инцидентов; способности финансовой организации обеспечить выполнение обязательств по защите интересов клиентов; способности финансовой организации осуществлять финансовые (банковские) операции, в том числе операции по переводу денежных средств в рамках срока исполнения обязательств, а также обеспечивать завершенность расчетов по таким операциям; способности финансовой организации возобновить предоставление финансовых и (или) информационных услуг в течение установленного времени после нарушения в работе	Н	О	О
ВИО.19.3	- оценки зрелости процессов планирования, реализации, контроля и совершенствования системы управления, определенной в рамках семейства стандартов ОН комплекса стандартов, в части выявления, регистрации, реагирования на инциденты и восстановления после их реализации	О	О	О
ВИО.19.4	- прогнозных оценок запланированных и незапланированных потерь от реализации инцидентов: на основе данных внутренней отчетности о фактических потерях за определенный временной период (запланированные потери); на основе сценариев в маловероятных, но возможных стрессовых ситуациях (незапланированные потери)	Н	Н	О
ВИО.19.5	- оценки способности финансовой организации обеспечить соблюдение требований законодательства Российской Федерации в области защиты информации, устанавливаемых на основании статей 57.4 и 76.4-1 Федерального закона [1], части 3 статьи 27 Федерального закона [11], а также устанавливаемых статьей 19 Федерального закона [12], статьей 16 Федерального закона [13] и Федеральным законом [14]	О	О	О

Окончание таблицы 9

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВИО.20	Определение способов проведения оценки уровня риска реализации информационных угроз	О	О	О
ВИО.21	Оценка риска реализации информационных угроз, которому финансовая организация подвергает или подвергается со стороны причастных сторон (за исключением клиентов финансовой организации), с учетом степени взаимосвязи и взаимозависимости между финансовой организацией и причастными сторонами (за исключением клиентов финансовой организации), в том числе степени взаимосвязи и взаимозависимости между их объектами информатизации	Н	О	О
ВИО.22	Организация и выполнение деятельности по переоценке риска реализации информационных угроз на основе: - результатов пересмотра модели информационных угроз; - информации о новом идентифицированном риске реализации информационных угроз; - выявленных событий риска реализации информационных угроз	О	О	О
* Финансовым организациям рекомендуется применять количественный способ при реализации данной меры. ** В случае если требования нормативных актов Банка России не устанавливают обязанность финансовой организации проведения количественной оценки риска [6] соответствующим способом, финансовым организациям рекомендуется применять количественный способ при реализации данной меры.				

8.2.3 Процесс «Организация ресурсного (кадрового и финансового) обеспечения»

8.2.3.1 Применяемые финансовой организацией меры по организации ресурсного (кадрового и финансового) обеспечения должны обеспечивать:

- организацию ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз;
- организацию ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ;
- организацию целевого обучения по вопросам выявления и противостояния реализации информационных угроз.

При реализации процесса «Организация ресурсного (кадрового и финансового) обеспечения» рекомендуется использовать [22].

8.2.3.2 Состав мер по организации ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 10.

Таблица 10 — Состав мер по организации ресурсного (кадрового и финансового) обеспечения процессов системы управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.1	Установление во внутренних документах финансовой организации методики оценки необходимого ресурсного (кадрового и финансового) обеспечения процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О

Продолжение таблицы 10

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.2	Организация и выполнение деятельности по оценке необходимого ресурсного (кадрового и финансового) обеспечения для определения состава основных ресурсов, необходимых в рамках процессов планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, в том числе:	—	—	—
ОРО.2.1	- для реализации функций в рамках управления риском реализации информационных угроз подразделений, формирующих «три линии защиты»	О	О	О
ОРО.2.2	- для обеспечения своевременного выявления, реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после их реализации	О	О	О
ОРО.3	Утверждение и пересмотр на регулярной основе исполнительным органом финансовой организации состава основных ресурсов	О	О	О
ОРО.4	Организация и выполнение деятельности по обеспечению состава основных ресурсов и удовлетворение потребностей: - в финансировании реализации и контроля процессов обеспечения операционной надежности и защиты информации; - в закупке или разработке соответствующих программных, аппаратных и (или) программно-аппаратных продуктов; - в привлечении поставщиков услуг; - в доступе к информационным ресурсам (источникам информации), который предоставляется на основе возмездного договора	О	О	О
ОРО.5	Организация кадрового обеспечения в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации:	—	—	—
ОРО.5.1	- установление требований на основе профессиональных стандартов к квалификации работников, в том числе профессионального стандарта для специалистов по информационной безопасности в кредитно-финансовой сфере	О	О	О
ОРО.5.2	- проведение оценки соответствия кандидатов на должности согласно установленным требованиям в отношении их компетенции	О	О	О
ОРО.6	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния кадровых рисков в рамках деятельности по управлению риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, учитывающих в том числе: - возможность ухода работников, задействованных при выполнении ключевых ролей по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации; - возможность возникновения конфликта интересов при выполнении ролей по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации*	О	О	О
ОРО.7	Организация и выполнение деятельности по оценке эффективности работников, задействованных в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации**	О	О	О

Окончание таблицы 10

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.8	Организация и выполнение деятельности по повышению эффективности работников, направленной на исправление недостатков, выявленных по результатам оценки, предусмотренной мерой ОРО.7 настоящей таблицы, и осуществление последующего контроля	О	О	О
* Снижение возможности возникновения конфликта интересов при выполнении ролей по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации посредством разделения (везде, где это возможно) ролей, связанных с реализацией и контролем за реализацией процессов. ** Допускается, если реализация меры ОРО.7 (и ОРО.8) будет произведена только в отношении отдельных категорий должностей, связанных с выполнением ключевых ролей в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации. Для отдельных таких категорий должностей рекомендуется устанавливать ключевые показатели эффективности в целях последующего контроля за их достижением.			

8.2.3.3 Состав мер по организации ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ применительно к уровням защиты приведен в таблице 11.

Таблица 11 — Состав мер по организации ресурсного (кадрового и финансового) обеспечения функционирования службы ИБ

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.9	Определение и обеспечение необходимой численности и требуемой компетенции работников при организации ресурсного (кадрового и финансового) обеспечения службы ИБ на основании: - анализа задач и функций, связанных с выполнением планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз, а также процессов систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, возложенных на службу ИБ; - уровня автоматизации процессов обеспечения операционной надежности и защиты информации; - прогноза возможного расширения состава задач и функций, возложенных на службу ИБ, в результате развития бизнес- и технологических процессов в соответствии с общей стратегией развития финансовой организации	О	О	О
ОРО.10	Определение минимальной необходимой численности работников службы ИБ с учетом: - трудозатрат на выполнение задач и функций, связанных с выполнением планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз, а также процессов систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, возложенных на службу ИБ; - размеров финансовой организации, количества филиалов (региональных представительств) и их территориального распределения; - количества работников финансовой организации, задействованных в выполнении бизнес- и технологических процессов	О	О	О
ОРО.11	Определение требований к квалификации работников службы ИБ на основании характеристик квалификации, которые содержатся в профессиональном стандарте специалистов по информационной безопасности в кредитно-финансовой сфере, с учетом особенностей выполняемых работниками трудовых функций, обусловленных применяемыми технологиями и способами организации производства и труда	О	О	О

Окончание таблицы 11

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.12	Определение требований в отношении компетенции работников службы ИБ с учетом: - наличия высшего профессионального образования в области ИБ и (или) информационных технологий; - наличия подтверждения соответствия квалификационным требованиям, устанавливаемым профессиональным стандартом специалистов по информационной безопасности в кредитно-финансовой сфере; - регулярного прохождения дополнительного (специализированного) обучения, переподготовки (повышения квалификации) в области ИБ	О	О	О
ОРО.13	Утверждение коллегиальным исполнительным органом финансовой организации ресурсов службы ИБ с целью выполнения задач и функций, связанных с планированием, реализацией, контролем и совершенствованием системы управления риском реализации информационных угроз, а также процессов систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, возложенных на службу ИБ	О	О	О
ОРО.14	Предоставление службе ИБ собственного бюджета, достаточного для целей выполнения задач и функций, связанных с выполнением процессов планирования, реализации, контроля и совершенствования системы управления риском реализации информационных угроз, а также систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, возложенных на службу ИБ	Н	О	О
ОРО.15	Определение в качестве куратора службы ИБ должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз	—	—	—
ОРО.16	Выделение на местах, в случае наличия у финансовой организации филиалов (региональных представительств), соответствующих подразделений ИБ (уполномоченных лиц) и организация их ресурсного (кадрового и финансового) обеспечения и обеспечение нормативной базой*	Н	О	О

* В случае централизации деятельности по управлению риском реализации информационных угроз, обеспечению операционной надежности и защиты информации финансовая организация определяет:

- необходимость в ресурсном (кадровом и финансовом) обеспечении соответствующих подразделений (уполномоченных лиц) с учетом функций, делегированных таким подразделениям (уполномоченным лицам);

- способ обеспечения нормативной базой соответствующих подразделений (уполномоченных лиц) — применение единой нормативной базы или разработка отдельных нормативных документов, отражающих специфику филиалов (региональных представительств).

8.2.3.4 Состав мер по организации целевого обучения по вопросам выявления и противостояния реализации информационных угроз применительно к уровням защиты приведен в таблице 12.

Таблица 12 — Состав мер по организации целевого обучения по вопросам выявления и противостояния реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОРО.17	Организация целевого обучения работников, задействованных в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, в частности организация целевого обучения по вопросам противостояния реализации информационных угроз для работников, входящих в группы повышенного риска*	Н	О	О
ОРО.18	Включение в разрабатываемые программы целевого обучения по вопросам выявления и противостояния реализации информационных угроз: - практических занятий, в рамках которых отрабатываются вопросы выявления индикаторов раннего обнаружения реализации информационных угроз (индикаторов (фактов) компрометации объектов информатизации) и реагирования на них; - практических занятий, в рамках которых отрабатываются вопросы противостояния реализации информационных угроз на основе возможных сценариев реализации информационных угроз; - практических занятий, в рамках которых отрабатываются вопросы восстановления после реализации инцидентов, связанных с реализацией информационных угроз, в том числе сбора и анализа технических данных (свидетельств)	Н	О	О
* К таким группам следует относить работников, обладающих привилегированным логическим доступом к объектам информатизации, задействованным в выполнении бизнес- и технологических процессов, входящих в критичную архитектуру.				

8.3 Направление 2 «Реализация системы управления риском реализации информационных угроз»

8.3.1 Процесс «Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз»

8.3.1.1 Подпроцесс «Разработка мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз»

Применяемые финансовой организацией меры по разработке мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз, должны обеспечивать:

- выбор и применение способа реагирования на риск реализации информационных угроз;
- разработку мероприятий, направленных на снижение СВР инцидентов;
- разработку мероприятий, направленных на ограничение СТП инцидентов.

При реализации процесса «Выбор и применение способа реагирования на риск реализации информационных угроз» рекомендуется использовать ГОСТ Р ИСО 31000, ГОСТ Р 27005.

Состав мер по выбору и применению способа реагирования на риск реализации информационных угроз применительно к уровням защиты приведен в таблице 13.

Таблица 13 — Состав мер по выбору и применению способа реагирования на риск реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
РМ.1	Выбор финансовой организацией способа реагирования на риск реализации информационных угроз по результатам оценки риска: - уклонение от риска, предусматривающее отказ финансовой организации от выполнения отдельных бизнес- и технологических процессов (оказания соответствующего вида услуг и операций) в связи с высоким уровнем риска; - передача риска, предусматривающая страхование, передача риска причастной стороне; - принятие риска, предусматривающее готовность финансовой организации принять запланированные и незапланированные потери в рамках установленных сигнальных и контрольных значений КПУР (лимита потерь, с соответствующей процедурой контроля соблюдения такого лимита), а также на основе мотивированного суждения финансовой организации о достаточности выделяемого капитала, необходимого на покрытие потерь от реализации риска реализации информационных угроз; - разработка и реализация мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	О	О	О
РМ.2	Разработка плана реагирования на риск реализации информационных угроз, обеспечивающего достижение и поддержание допустимого уровня такого риска (риск-аппетита финансовой организации)	О	О	О
РМ.3	Определение в плане реагирования на риск реализации информационных угроз группы КПУР*, характеризующих уровень зрелости процессов обеспечения:	—	—	—
РМ.3.1	- применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов [8] — [10], [21]	Н	О	О
РМ.3.2	- реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня [8] — [10]	Н	О	О
РМ.3.3	- планирования, реализации, контроля и совершенствования системы защиты информации, требования к которой определены национальными стандартами семейства ЗИ комплекса стандартов	О	О	О
РМ.3.4	- планирования, реализации, контроля и совершенствования системы обеспечения операционной надежности, требования к которой определены национальными стандартами семейства ОН комплекса стандартов	О	О	О
РМ.4	Определение в рамках плана реагирования на риск реализации информационных угроз сигнальных и контрольных значений КПУР*, предусмотренных мерой РМ.3 настоящей таблицы, с учетом допустимого уровня такого риска (риск-аппетита)	О	О	О
РМ.5	Утверждение плана реагирования на риск реализации информационных угроз исполнительным органом финансовой организации и (или) должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз	О	О	О
* Состав КПУР по указанной группе, а также их сигнальные и контрольные значения приведены в приложениях Д, Е.				

Состав мер по разработке мероприятий, направленных на снижение СВР инцидентов, применительно к уровням защиты приведен в таблице 14.

Таблица 14 — Состав мер по разработке мероприятий, направленных на снижение СВР инцидентов

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
РМ.6	Планирование процессов применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов, входящих в критичную архитектуру [8]—[10], [21]	Н	О	О
РМ.7	Планирование процессов реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня [8]—[10]	Н	О	О
РМ.8	Планирование процессов применения организационных и технических мер, направленных на реализацию требований к процессам систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, включая:	—	—	—
РМ.8.1	- планирование применения организационных и технических мер, направленных на реализацию требований к процессам системы защиты информации, определенной в рамках семейства стандартов ЗИ комплекса стандартов	О	О	О
РМ.8.2	- планирование применения организационных и технических мер, направленных на реализацию требований к процессам системы обеспечения операционной надежности, определенной в рамках семейства стандартов ОН комплекса стандартов	О	О	О
РМ.9	Планирование процессов применения организационных и технических мер, предусмотренных мерой РМ.8 настоящей таблицы, включающее: - формирование состава (выбор) мер*, обеспечивающих соблюдение сигнальных и контрольных значений КПУР, принятых финансовой организацией; - исключение из выбранного состава мер, не связанных с используемыми информационными технологиями	О	О	О
РМ.9	- адаптацию (уточнение), при необходимости, выбранного состава мер с учетом результатов проведения идентификации критичной архитектуры, а также результатов моделирования информационных угроз; - дополнение адаптированного (уточненного) состава мерами, которые необходимы для обработки информационных угроз, закрепленных в модели угроз безопасности информации финансовой организации, в том числе обеспечения выполнения требований, установленных нормативными правовыми актами [23]—[26]	О	О	О
РМ.10	Определение приоритетов реализации процессов, планируемых в рамках реализации мер РМ.6 — РМ.9 настоящей таблицы, в отношении каждого бизнес- и технологического процесса, входящего в критичную архитектуру	О	О	О

* При невозможности технической реализации отдельных выбранных мер, а также с учетом экономической целесообразности на этапах адаптации (уточнения) выбранного состава мер могут разрабатываться иные (компенсирующие) меры на основании мотивированного суждения финансовой организации.

Компенсирующие меры должны быть направлены на предотвращение (снижение вероятности) реализации тех же информационных угроз, на нейтрализацию которых направлены меры из выбранного состава мер, не применяемые в связи с невозможностью технической реализации и (или) экономической целесообразностью.

В случае нереализации компенсирующих мер финансовая организация должна принять меры по страхованию запланированных и незапланированных финансовых потерь в результате реализации информационных угроз, на нейтрализацию которых направлены меры из выбранного состава мер, не применяемые в связи с невозможностью технической реализации и (или) экономической целесообразностью, и (или) учету указанных потерь при расчете капитала, необходимого на покрытие потерь от реализации риска реализации информационных угроз (в составе операционного риска).

Состав мер по разработке мероприятий, направленных на ограничение СТП инцидентов, применительно к уровням защиты приведен в таблице 15.

Таблица 15 — Состав мер по разработке мероприятий, направленных на ограничение СТП инцидентов

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
РМ.11	Определение ограничений по параметрам финансовых (банковских) операций, в том числе переводов денежных средств [10]	Н	О	О
РМ.12	Определение способа и порядка возмещения потерь от реализации инцидентов, в том числе за счет резервов на запланированные и незапланированные потери и (или) посредством переноса риска на участников финансового рынка (страхования)	Н	О	О
РМ.13	Планирование применения организационных и технических мер, направленных на реализацию требований к процессам системы обеспечения операционной надежности, определенной в рамках семейства стандартов ОН комплекса стандартов, в части: - поддержания непрерывности выполнения бизнес- и технологических процессов; - выявления, реагирования на инциденты и восстановления после их реализации	О	О	О

8.3.1.2 Подпроцесс «Защита от информационных угроз»

Применяемые финансовой организацией меры по защите от информационных угроз должны обеспечивать:

- защиту информации финансовой организации[1)];
- операционную надежность;
- управление риском реализации информационных угроз при аутсорсинге и взаимодействии с поставщиками услуг;
- управление риском внутреннего нарушителя.

Примечание — В настоящем стандарте рассматривается часть деятельности по управлению риском, связанная с принятием мер, направленных на нейтрализацию информационных угроз (снижением СВР и ограничением СТП от реализации информационных угроз), связанных с внутренним нарушителем;

- управление риском реализации информационных угроз в финансовой экосистеме;
- выполнение мероприятий, направленных на предотвращение утечек информации[2)].

При реализации процесса «Защита от информационных угроз» следует использовать ГОСТ Р 57580.1, ГОСТ Р 57580.4. В частности, при реализации требования к управлению риском реализации информационных угроз при аутсорсинге рекомендуется использовать ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, а также [27].

Состав мер по обеспечению защиты информации финансовой организации применительно к уровням защиты приведен в таблице 16.

Таблица 16 — Состав мер по защите информации финансовой организации

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.1	Реализация, контроль и совершенствование процессов применения технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов [8]—[10], [21], планирование которых предусмотрено мерой РМ.6 таблицы 14	Н	О	О

[1)] В целях обеспечения безопасности финансовых (банковских) операций согласно ГОСТ Р 57580.1.

[2)] Не контролируемое финансовой организацией распространение информации конфиденциального характера.

Окончание таблицы 16

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.2	Реализация, контроль и совершенствование процессов реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня [8]—[10], планирование которых предусмотрено мерой РМ.7 таблицы 14	Н	О	О
ЗИУ.3	Реализация, контроль и совершенствование процессов системы защиты информации, определяемой в рамках семейства стандартов ЗИ комплекса стандартов, планирование которых предусмотрено мерой РМ.8.1 таблицы 14	О	О	О
ЗИУ.4	Определение во внутренних документах требований к внедрению процессов, предусмотренных мерами ЗИУ 1 — ЗИУ.3 настоящей таблицы, на этапах жизненного цикла* объектов информатизации финансовой организации, начиная с этапа «Создание», способом, обеспечивающим заданный уровень защиты информации на этапах «Ввод в эксплуатацию» и «Эксплуатация (сопровождение)» в отношении:	—	—	—
ЗИУ.4.1	- процессов, предусмотренных мерами ЗИУ.1, ЗИУ.2 настоящей таблицы	Н	О	О
ЗИУ.4.2	- процессов, предусмотренных мерами ЗИУ.3 настоящей таблицы	О	О	О
ЗИУ.5	Реализация принципа обеспечения защиты информации, предусматривающего выделение контуров безопасности согласно ГОСТ Р 57580.1**	О	О	О
ЗИУ.6	Обеспечение необходимого уровня зрелости процессов, предусмотренных мерами ЗИУ.1 — ЗИУ.3 настоящей таблицы, согласно принятым финансовой организацией сигнальным и контрольным значениям КПУР, предусмотренным мерой РМ.4 таблицы 13	Н	О	О
*Определяемых согласно ГОСТ Р 57580.1. **Выполнение мер защиты информации, приведенных в ГОСТ Р 57580.1, предусматривающих выделение контуров безопасности, с учетом топологии внутренней вычислительной сети, потоков защищаемой информации (внутренних и внешних).				

Состав мер по обеспечению операционной надежности применительно к уровням защиты приведен в таблице 17.

Таблица 17 — Состав мер по обеспечению операционной надежности

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.7	Реализация, контроль и совершенствование процессов системы обеспечения операционной надежности, определенной в рамках семейства стандартов ОН комплекса стандартов, планирование которых предусмотрено мерой РМ.8.2 таблицы 14	О	О	О
ЗИУ.8	Определение во внутренних документах требований к внедрению процессов, предусмотренных мерой ЗИУ.7 настоящей таблицы, на этапах жизненного цикла* объектов информатизации финансовой организации, начиная с этапа «Создание», способом, обеспечивающим заданный уровень защиты на этапах «Ввод в эксплуатацию» и «Эксплуатация (сопровождение)»	О	О	О
ЗИУ.9	Обеспечение необходимого уровня зрелости процессов, предусмотренных мерой ЗИУ.7 настоящей таблицы, согласно принятым финансовой организацией сигнальным и контрольным значениям КПУР, предусмотренным мерой РМ.4 таблицы 13	Н	О	О
* Определяемых согласно ГОСТ Р 57580.1.				

Состав мер по управлению риском реализации информационных угроз при аутсорсинге применительно к уровням защиты приведен в таблице 18.

Таблица 18 — Состав мер по управлению риском реализации информационных угроз при аутсорсинге

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.10	Определение вопросов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации в рамках политики аутсорсинга, утверждаемой советом директоров (наблюдательным советом) или коллегиальным исполнительным органом финансовой организации	О	О	О
ЗИУ.11	Отнесение к зоне компетенции коллегиального исполнительного органа (а в случае его отсутствия — единоличного исполнительного органа) или подотчетных им коллегиальных органов финансовой организации вопросов, связанных с управлением риском реализации информационных угроз при аутсорсинге	О	О	О
ЗИУ.12	Организация и выполнение деятельности по выявлению и идентификации риска реализации информационных угроз, а также его оценке при аутсорсинге*	О	О	О
ЗИУ.13	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз при аутсорсинге	О	О	О
ЗИУ.14	Организация и выполнение деятельности по мониторингу риска реализации информационных угроз при аутсорсинге	О	О	О
ЗИУ.15	Организация и выполнение деятельности по обеспечению соответствия фактических значений КПУР принятым финансовой организацией, предусмотренных мерой ОПР.11 таблицы 5, при аутсорсинге	О	О	О
ЗИУ.16	Применение, в случае передачи на аутсорсинг процессов обеспечения операционной надежности и защиты информации финансовой организации, соглашений об уровне предоставления услуг (Service level agreement, SLA) и соглашения о неразглашении информации конфиденциального характера (Non-Disclosure Agreement, NDA) как дополнения к соглашению об аутсорсинге таких процессов	О	О	О
ЗИУ.17	Организация и выполнение деятельности по контролю со стороны финансовой организации качества услуг аутсорсинга процессов обеспечения операционной надежности и защиты информации на основе соглашений об уровне предоставления услуг (Service level agreement, SLA)	О	О	О
* При организации и выполнении деятельности по выявлению и идентификации риска реализации информационных угроз, а также его оценки при привлечении поставщика облачных услуг наряду с [27] рекомендуется использовать ГОСТ Р ИСО/МЭК 27036-4.				

Состав мер по управлению риском внутреннего нарушителя применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

Состав мер по управлению риском реализации информационных угроз в финансовой экосистеме применительно к уровням защиты приведен в таблице 19.

Таблица 19 — Состав мер по управлению риском реализации информационных угроз в финансовой экосистеме

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.17	Определение в рамках финансовой экосистемы правил и требований к участникам финансовой экосистемы (за исключением пользователей финансовой экосистемы) в части управления риском реализации информационных угроз:	О	О	О
ЗИУ.17.1	- правил и требований к установлению и соблюдению поставщиками финансовых услуг состава КПУР, предусмотренных мерой ОПР.11 таблицы 5, при предоставлении финансовых и (или) информационных услуг в рамках финансовой экосистемы	О	О	О
ЗИУ.17.2	- правил и требований к выявлению и идентификации риска реализации информационных угроз, а также его оценки поставщиками финансовых услуг	О	О	О
ЗИУ.17.3	- правил и требований к применению участниками финансовой экосистемы (за исключением пользователей финансовой экосистемы) технологических мер защиты информации, реализуемых на технологических участках бизнес- и технологических процессов в рамках финансовой экосистемы, включая идентификацию и аутентификацию пользователей финансовой экосистемы* (в том числе предоставляемые поставщиком облачных услуг)	О	О	О
ЗИУ.17.4	- правил и требований к планированию, реализации, контролю и совершенствованию участниками финансовой экосистемы (за исключением пользователей финансовой экосистемы) процессов системы управления, определяемых в рамках семейств стандартов ОН и ЗИ комплекса стандартов**	О	О	О
ЗИУ.17.5	- правил и требований к реализации мероприятий, направленных на предотвращение утечек информации***	О	О	О
ЗИУ.17.6	- правил и требований к безопасности раскрытия информации конфиденциального характера, относящейся к пользователям финансовой экосистемы, внутри финансовой экосистемы*[4]	О	О	О
ЗИУ.17.7	- правил и требований к выявлению событий риска реализации информационных угроз, в том числе к сбору и регистрации информации о событиях риска реализации информационных угроз и потерях в рамках финансовой экосистемы	О	О	О
ЗИУ.17.8	- правил и требований к реагированию на инциденты и восстановлению функционирования бизнес- и технологических процессов и объектов информатизации после их реализации, в том числе к взаимодействию между участниками финансовой экосистемы при реагировании и восстановлении после реализации таких инцидентов	О	О	О
ЗИУ.17.9	- правил и требований к обеспечению осведомленности об актуальных информационных угрозах, в том числе пользователей финансовой экосистемы	О	О	О
ЗИУ.17.10	- правил и требований к мониторингу риска реализации информационных угроз в рамках финансовой экосистемы	О	О	О

Окончание таблицы 19

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ЗИУ.18	Рассмотрение в рамках выявления и идентификации риска реализации информационных угроз, а также его оценки в рамках финансовой экосистемы следующих дополнительных видов такого риска: - риска реализации информационных угроз, связанного с нарушением обеспечения операционной надежности бизнес- и технологических процессов в рамках финансовой экосистемы; - риска реализации информационных угроз, связанного с неконтролируемым участниками финансовой экосистемы распространением информации конфиденциального характера (утечками информации); - риска реализации информационных угроз, связанного с осуществлением финансовых (банковских) операций, в том числе операций по переводу денежных средств без согласия пользователей финансовой экосистемы	О	О	О
* В частности, идентификация устройств пользователей финансовой экосистемы (цифровой отпечаток устройства — device fingerprint) в целях формирования и (или) применения в рамках финансовой экосистемы дополнительных контрольных параметров для авторизации пользователей при их обращении за предоставлением финансовых услуг. ** Как минимум в отношении модулей, обеспечивающих интеграционное взаимодействие объектов информатизации участников финансовой экосистемы (за исключением пользователей финансовой экосистемы). *** Неконтролируемого участниками финансовой экосистемы распространения информации конфиденциального характера. *4 В частности, применение прикладных программных интерфейсов, обеспечивающих безопасность финансовых сервисов на основе протокола OpenID [28], [29].				

Состав мер по выполнению мероприятий, направленных на предотвращение утечек информации, применительно к уровням защиты приведен в рамках семейства ЗИ комплекса стандартов — процессы «Обеспечение защиты информации при управлении доступом» и «Предотвращение утечек информации».

8.3.1.3 Подпроцесс «Реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации»[1)]

Применяемые финансовой организацией меры по реагированию на инциденты и восстановлению после их реализации должны обеспечивать:

- реагирование на инциденты в отношении критичной архитектуры;
- восстановление выполнения бизнес- и технологических процессов и функционирования объектов информатизации после реализации инцидентов;
- проведение анализа причин и последствий реализации инцидентов;
- организацию взаимодействия между подразделениями финансовой организации, а также между финансовой организацией и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов.

Состав мер по реагированию на инциденты в отношении критичной архитектуры применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов. Процесс «Управление инцидентами защиты информации», приведенный в ГОСТ Р 57580.1, является составной частью реагирования на инциденты в отношении критичной архитектуры, его реализация должна быть дополнена соответствующими мерами, определенными в рамках семейства ОН комплекса стандартов, на случаи реализации инцидентов защиты информации в отношении критичной архитектуры.

[1)] В настоящем стандарте данный процесс рассматривается в рамках управления риском реализации информационных угроз в качестве выполнения подготовительных мероприятий, обеспечивающих готовность финансовой организации противостоять реализации информационных угроз.

Состав мер по восстановлению функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

Состав мер по проведению анализа причин и последствий реализации инцидентов применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

Состав мер по организации взаимодействия между подразделениями финансовой организации, а также между финансовой организацией и Банком России, причастными сторонами в рамках реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.3.2 Процесс «Выявление событий риска реализации информационных угроз»

8.3.2.1 Применяемые финансовой организацией меры по выявлению событий риска реализации информационных угроз должны обеспечивать:

- сбор и регистрацию информации о внутренних событиях риска реализации информационных угроз и потерях;
- выявление и фиксацию инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации;
- ведение претензионной работы.

При реализации процесса «Защита от информационных угроз» рекомендуется использовать ГОСТ Р 57580.1, а также [30], [31].

8.3.2.2 Состав мер по сбору и регистрации информации о внутренних событиях риска реализации информационных угроз и потерях применительно к уровням защиты приведен в таблице 20.

Таблица 20 — Состав мер по сбору и регистрации информации о внутренних событиях риска реализации информационных угроз и потерях

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВСР.1	Организация и выполнение деятельности по выявлению и отнесению к событиям риска реализации информационных угроз результатов, получаемых в рамках: - выявления и регистрации инцидентов, в том числе обнаружение реализации компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации; - ведения претензионной работы; - реализации программ по мотивации работников к инициативному информированию о возможной реализации и выявленных инцидентах	О	О	О
ВСР.2	Классификация событий риска реализации информационных угроз с учетом 6.14, в том числе в соответствии с требованиями нормативных актов Банка России [6]	О	О	О
ВСР.3	Организация и выполнение деятельности по ведению базы событий риска реализации информационных угроз, включая:	—	—	—
ВСР.3.1	- определение порядка ведения базы событий*	О	О	О
ВСР.3.2	- определение порядка установления величины потерь от реализации события риска реализации информационных угроз, при которой осуществляется регистрация таких событий в базе событий (порог регистрации), в том числе в соответствии с требованиями нормативных актов Банка России [6]	О	О	О
ВСР.3.3	- определение перечня ролей и ответственных по ведению базы событий	О	О	О
ВСР.3.4	- определение порядка контроля за своевременностью отражения потерь от реализации событий риска реализации информационных угроз	О	О	О

Окончание таблицы 20

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВСР.3.5	- хранение в базе событий информации о выявленных событиях риска реализации информационных угроз, в том числе сведений о проведении их анализа не менее трех лет**	Т	Н	Н
ВСР.3.6	- хранение в базе событий информации о выявленных событиях риска реализации информационных угроз, в том числе сведений о проведении их анализа не менее пяти лет**	Н	Т	Т
ВСР.3.7	- обеспечение целостности и доступности данных, содержащихся в базе событий, а также сохранности данных о потерях и возмещениях***	Т	Т	Т
ВСР.3.8	- протоколирование и контроль внесения изменений в базу событий	Т	Т	Т
ВСР.4	Организация и выполнение деятельности по регистрации информации о выявленных событиях риска реализации информационных угроз и потерях*[4] в базе событий такого риска с учетом их классификации и порога регистрации, в том числе в соответствии с требованиями нормативных актов Банка России [6]	О	О	О
ВСР.5	Организация и выполнение деятельности по определению потерь от реализации событий риска реализации информационных угроз и возмещений, в том числе в соответствии с требованиями нормативных актов Банка России [6], включая:	—	—	—
ВСР.5.1	- учет потерь, установление сроков выявления и правил отражения в бухгалтерском учете	О	О	О
ВСР.5.2	- установление порядка и метода определения потерь (прямых, косвенных, качественных*[5])	О	О	О
ВСР.5.3	- определение потерь финансовой организации, причастных сторон, в том числе клиентов финансовой организации с учетом классификации согласно приложению Г, в том числе в соответствии с требованиями нормативных правовых актов Банка России [6]	О	О	О
ВСР.5.4	- установление порядка определения валовых и чистых (фактических) потерь от реализации событий риска реализации информационных угроз, в том числе в соответствии с требованиями нормативных актов Банка России [6]	О	О	О

* Как в общей базе событий, так и в отдельной базе событий риска реализации информационных угроз. В случае если финансовая организация ведет отдельную базу событий риска реализации информационных угроз, подразделению, ответственному за ее ведение (службе ИБ), следует обеспечить возможность ее синхронизации с базой событий операционного риска, в том числе в соответствии с требованиями нормативных актов Банка России [6] (в частности, с требованиями к классификации событий риска и требованиями к ведению такой базы).

** Если иной срок не установлен в нормативных актах Банка России [6].

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

*[4] Данные о событиях риска реализации информационных угроз и потерях должны охватывать виды деятельности финансовой организации, связанные с предоставлением финансовых и (или) информационных услуг, все структурные подразделения финансовой организации, объекты информатизации и регионы присутствия.

*[5] Финансовым организациям следует проводить оценку значимости качественных потерь в соответствии с установленной во внутренних документах финансовой организации шкалой качественных оценок (например, по четырехуровневой шкале: «очень высокие», «высокие», «средние», «низкие»).

8.3.2.3 Состав мер по выявлению и фиксации инцидентов, в том числе обнаружению реализации компьютерных атак, и выявлению фактов (индикаторов) компрометации объектов информатизации применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.3.2.4 Состав мер по ведению претензионной работы применительно к уровням защиты приведен в таблице 21.

Таблица 21 — Состав мер по ведению претензионной работы

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ВСР.6	Организация и выполнение деятельности по обработке обращений причастных сторон, в том числе клиентов финансовой организации, о выявлении ими событий риска реализации информационных угроз, включая события такого риска, связанные с осуществлением финансовых (банковских) операций, в том числе операций по переводу денежных средств без согласия клиентов	О	О	О
ВСР.7	Организация и выполнение деятельности по доведению до причастных сторон, в том числе клиентов финансовой организации, результатов проведения финансовой организацией анализа по факту их обращений	О	О	О

8.3.3 Процесс «Обеспечение осведомленности об актуальных информационных угрозах»

8.3.3.1 Применяемые финансовой организацией меры по обеспечению осведомленности об актуальных информационных угрозах должны обеспечивать:

- организацию взаимодействия финансовой организации и причастных сторон, в том числе клиентов финансовой организации, при обмене информацией об актуальных сценариях реализации информационных угроз;
- использование информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации;
- повышение осведомленности работников финансовой организации в части противостояния реализации информационных угроз.

8.3.3.2 Состав мер по организации взаимодействия финансовой организации и причастных сторон, в том числе клиентов финансовой организации, при обмене информацией об актуальных сценариях реализации информационных угроз применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.3.3.3 Состав мер по использованию информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.3.3.4 Состав мер по повышению осведомленности работников финансовой организации в части противостояния реализации информационных угроз применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.4 Направление 3 «Контроль системы управления риском реализации информационных угроз»

8.4.1 Процесс «Установление и реализация программ контроля и аудита»

8.4.1.1 Применяемые финансовой организацией меры по установлению и реализации программ контроля и аудита должны обеспечивать:

- проведение самооценки и профессиональной независимой оценки[1)] зрелости процессов обеспечения операционной надежности и защиты информации;
- проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения);

[1)] Обязательность проведения независимой профессиональной оценки устанавливается нормативными актами Банка России, в частности [8]—[10].

- оценку эффективности функционирования системы управления риском реализации информационных угроз;
- организацию внутренней отчетности в рамках управления риском реализации информационных угроз.

8.4.1.2 Состав мер по проведению самооценки и независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации применительно к уровням защиты приведен в таблице 22.

Таблица 22 — Состав мер по проведению самооценки и независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
УПК.1	Установление и реализация программы проведения самооценки зрелости процессов планирования, реализации, контроля и совершенствования систем управления, определенных в рамках семейств стандартов ОН и ЗИ комплекса стандартов, согласно соответствующим методикам оценки соответствия (далее — самооценка ОН и ЗИ)	О	Н	Н
УПК.2	Установление и реализация программы проведения независимой профессиональной оценки* зрелости процессов планирования, реализации, контроля и совершенствования систем управления, определенных в рамках семейств стандартов ОН и ЗИ Комплекса стандартов, согласно соответствующим методикам оценки соответствия (далее — аудиты ОН и ЗИ)	Н	О	О
УПК.3	Установление плана самооценки ОН и ЗИ для каждого проводимого аудита, определяющего: - цель самооценки ОН и ЗИ; - критерии самооценки ОН и ЗИ**; - область самооценки ОН и ЗИ; - дату и продолжительность проведения самооценки ОН и ЗИ; - состав аудиторской группы; - описание деятельности и мероприятий по проведению самооценки ОН и ЗИ; - распределение ресурсов при проведении самооценки ОН и ЗИ	О	Н	Н
УПК.4	Установление плана аудита ОН и ЗИ для каждого проводимого аудита, определяющего: - цель аудита ОН и ЗИ; - критерии аудита ОН и ЗИ**; - область аудита ОН и ЗИ; - дату и продолжительность проведения аудита ОН и ЗИ; - организацию, предоставляющую услуги внешнего аудита, и состав аудиторской группы; - описание деятельности и мероприятий по проведению аудита ОН и ЗИ; - распределение ресурсов при проведении аудита ОН и ЗИ	Н	О	О
УПК.5	Определение во внутренних документах правил привлечения организации, предоставляющей услуги внешнего аудита, при проведении аудитов ОН и ЗИ***	Н	О	О
УПК.6	Фиксация результатов проведения самооценок и аудитов ОН и ЗИ в виде отчетов, содержащих мотивированное суждение об уровне зрелости процессов совершенствования систем управления, определенных в рамках семейств стандартов ОН и ЗИ Комплекса стандартов, согласно соответствующим методикам оценки соответствия	О*[4]	О	О

Окончание таблицы 22

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
УПК.7	Доведение результатов самооценок и аудитов ОН и ЗИ до совета директоров (наблюдательного совета) и исполнительного органа финансовой организации, а также должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз	О*4	О	О
УПК.8	Организация и выполнение деятельности по хранению, предоставлению санкционированного доступа и использованию материалов (в частности, отчетов), получаемых в процессе проведения самооценок и аудитов ОН и ЗИ	О*4	О	О

* Обязательность проведения независимой профессиональной оценки устанавливается нормативными актами Банка России, в частности [8] — [10].

** Совокупность требований к составу и содержанию мер обеспечения операционной надежности и защиты информации, определенных в соответствии с ГОСТ Р 57580.4 и ГОСТ Р 57580.1 соответственно.

*** Рекомендуется для проведения внешнего аудита привлекать организации, подтвердившие соответствие своей деятельности ГОСТ Р ИСО/МЭК 27006 и ГОСТ Р ИСО/МЭК 17021-1.

*4 Мера применяется только в отношении самооценки ОН и ЗИ.

8.4.1.3 Состав мер по проведению сценарного анализа (в части возможной реализации информационных угроз) и тестированию (с использованием его результатов) готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения) применительно к уровням защиты приведен в рамках семейства стандартов ОН комплекса стандартов.

8.4.1.4 Состав мер по оценке эффективности функционирования системы управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 23.

Таблица 23 — Состав мер по оценке эффективности функционирования системы управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
УПК.9	Организация и выполнение деятельности по оценке фактических значений КПУР на основе:	—	—	—
УПК.9.1	- данных, содержащихся в базе событий риска реализации информационных угроз	О	О	О
УПК.9.2	- результатов самооценок ОН и ЗИ*	О	Н	Н
УПК.9.3	- результатов аудитов ОН и ЗИ	Н	О	О
УПК.9.4	- результатов сценарного анализа и тестирования готовности финансовой организации противостоять реализации информационных угроз	Н	Н	О
УПК.9.5	- результатов оценки эффективности функционирования системы управления риском реализации информационных угроз, проводимой подразделением, формирующим «третью линию защиты»	О	О	О
УПК.10	Определение во внутренних документах:	—	—	—
УПК.10.1	- порядка оценки подразделением, формирующим «третью линию защиты», и (или) внешним аудитором эффективности функционирования системы управления риском реализации информационных угроз, в том числе выполнения процессов управления таким риском	О	О	О

Окончание таблицы 23

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
УПК.10.2	- порядка привлечения для оценки эффективности функционирования системы управления риском реализации информационных угроз внешних аудиторов или экспертов	Н	Н	Н
УПК.11	Проведение ежегодной оценки эффективности функционирования системы управления риском реализации информационных угроз подразделением, формирующим «третью линию защиты», включая оценку:	—	—	—
УПК.11.1	- полноты и точности информации, отраженной в базе событий риска реализации информационных угроз, а также корректности ведения такой базы	Н	О	О
УПК.11.2	- соблюдения установленных финансовой организацией в политике управления риском реализации информационных значений КПУР	Н	О	О
УПК.11.3	- корректности определения вида и величины потерь от реализации событий риска реализации информационных угроз (в составе операционного риска)	Н	О	О
УПК.11.4	- корректности проведенных оценок величины потерь от реализации риска реализации информационных угроз	Н	О	О
УПК.11.5	- мероприятий, направленных на уменьшение негативного влияния риска реализации информационных угроз	Н	О	О
УПК.12	Представление на рассмотрение фактических значений КПУР на регулярной основе или в случае выявления факта превышения сигнального и (или) контрольного значения одного из КПУР: - совету директоров (наблюдательному совету) финансовой организации не реже одного раза в год; - исполнительному органу финансовой организации, в том числе должностному лицу, ответственному за функционирование системы управления риском реализации информационных угроз, не реже одного раза в квартал	Н	О	О
* Самооценка проводится с привлечением службы ИБ (по решению финансовой организации может проводиться с привлечением внешнего аудитора).				

8.4.1.5 Состав мер по организации внутренней отчетности в рамках управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 24.

Таблица 24 — Состав мер по организации внутренней отчетности в рамках управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
УПК.13	Формирование внутренней отчетности финансовой организации: - о результатах выявления и идентификации риска реализации информационных угроз, его оценки, а также о выбранном способе реагирования на такой риск; - о планируемых и реализованных мероприятиях, направленных на уменьшение негативного влияния риска реализации информационных угроз; - о выявленных событиях риска реализации информационных угроз; - о результатах реагирования на инциденты и восстановления после их реализации, в том числе анализа причин и последствий реализации таких инцидентов; - о результатах реализации планов по обучению и повышению осведомленности работников финансовой организации в части противостояния реализации информационных угроз; о результатах оценок необходимого ресурсного (кадрового и финансового) обеспечения; - о результатах реализации программ контроля и аудита, в том числе фактических значениях КПУР, а также мониторинга риска реализации информационных угроз (включая фактические значения КИР и результаты оценки потенциала превышения сигнальных и контрольных значений КПУР); - о результатах анализа необходимости совершенствования системы управления риском реализации информационных угроз, принятых решениях по совершенствованию системы управления риском реализации информационных угроз (включая предпринятые тактические или стратегические улучшения системы управления риском реализации информационных угроз)	О	О	О
УПК.14	Включение в отчетность о выявленных событиях риска реализации информационных угроз сведений о ведении претензионной работы финансовой организации в отношении ее причастных сторон, в том числе клиентов финансовой организации	О	О	О
УПК.15	Включение в отчетность о результатах мониторинга риска реализации информационных угроз информации о реализовавшихся инцидентах, содержащей в том числе: - общее количество зафиксированных инцидентов за отчетный период; - общее количество зарегистрированных событий риска реализации информационных угроз за отчетный период; - сумму потерь от реализации инцидентов в финансовой организации; - сумму потерь от реализации инцидентов со стороны причастных сторон (за исключением клиентов финансовой организации)	О	О	О
УПК.16	Определение процедур информирования и состава отчетности для представления совету директоров (наблюдательному совету) и коллегиальному исполнительному органу (а в случае его отсутствия — единоличному исполнительному органу) финансовой организации в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации подразделениями финансовой организации, формирующими «три линии защиты»	Н	О	О
УПК.17	Организация и выполнение деятельности по валидации и верификации данных, содержащихся в отчетности, предусмотренной мерой УПК.16 настоящей таблицы, в рамках управления риском реализации информационных угроз, со стороны подразделений, формирующих «третью линию защиты»	Н	О	О

8.4.2 Процесс «Мониторинг риска реализации информационных угроз»

8.4.2.1 Финансовая организация должна применять меры по мониторингу риска реализации информационных угроз.

При реализации процесса «Мониторинг риска реализации информационных угроз» рекомендуется использовать ГОСТ Р ИСО 31000, ГОСТ Р ИСО/МЭК 27005.

8.4.2.2 Состав мер по мониторингу риска реализации информационных угроз применительно к уровням защиты приведен в таблице 25.

Таблица 25 — Состав мер по мониторингу риска реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
МР.1	Установление требований к КИР и их документированию, включающее: - количественное измерение КИР; способы расчета КИР, в том числе с использованием средств автоматизации; - периодичность (не реже одного раза в год) пересмотра КИР для поддержания КИР в актуальном состоянии; - регулярность и своевременность расчета КИР с установлением сроков (периодов) расчета КИР*; - валидацию КИР для проверки адекватности применяемого индикатора и подход к его расчету; - состав информации, используемой для расчета КИР, и ее источников, включая способ получения такой информации; - пороговые значения КИР с обоснованием их установления; - подразделения финансовой организации, ответственные за предоставление данных для расчета КИР и (или) расчет КИР; - порядок реагирования на превышение пороговых значений КИР, в том числе процедуры эскалации (в том числе информирования исполнительного органа финансовой организации и должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз)	Н	Н	О
МР.2	Определение в рамках установления требований к КИР, предусмотренных мерой МР.1 настоящей таблицы, в части состава информации, используемой для КИР расчета, наборов КИР в целях мониторинга возможного превышения сигнальных и (или) контрольных значений для каждой группы КПУР:	—	—	—
МР.2.1	- набора КИР, характеризующих динамику возникновения инцидентов, приведших к прямым и (или) непрямым потерям финансовой организации, для мониторинга группы КПУР, характеризующих уровень совокупных потерь в результате реализации информационных угроз	Н	Н	О
МР.2.2	- определения набора КИР, характеризующих динамику возникновения инцидентов, вызвавших прерывание выполнения бизнес- и технологических процессов, для мониторинга группы КПУР, характеризующих уровень операционной надежности бизнес- и технологических процессов финансовой организации	Н	Н	О
МР.2.3	- определения набора КИР, характеризующих динамику поступления уведомлений от клиентов финансовой организации об осуществлении финансовых (банковских) операций, в том числе операций по переводу денежных средств без их согласия, для мониторинга группы КПУР, характеризующих уровень несанкционированных операций (потерь клиентов финансовой организации) в результате инцидентов	Н	Н	О
МР.2.4	- определения набора КИР, характеризующих динамику выявленных нарушений** в рамках выполнения процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, для мониторинга группы КПУР, характеризующей уровень зрелости таких процессов	Н	Н	О

Окончание таблицы 25

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
МР.3	Определение в рамках установления требований к КИР, предусмотренных мерой МР.1 настоящей таблицы, в части источников информации, используемой для расчета КИР, следующих данных: - данных, формируемых подразделениями, формирующими «первую линию защиты»; - данных, формируемых в рамках ведения финансовой организацией претензионной работы; - данных, формируемых по результатам реализации программ контроля и аудита; - данных, формируемых по результатам оценки эффективности системы управления риском реализации информационных угроз	Н	Н	О
МР.4	Определение в рамках установления требований к КИР, предусмотренных мерой МР.1 настоящей таблицы, в части обоснования установления пороговых значений КИР, критериев учета влияния превышения пороговых значений КИР на возможность превышения сигнальных и контрольных значений КПУР	Н	Н	О
МР.5	Определение порядка информирования должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз, в случае выявления факта возможного превышения сигнальных и контрольных значений КПУР, о котором свидетельствуют фактические расчетные значений КИР	Н	Н	О
* Например, в постоянном режиме, один раз в неделю, по состоянию на момент закрытия операционного дня [6]. ** Обеспечение учета таких нарушений в случае их выявления вне проводимой самооценки и профессиональной независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации, а также вне проводимой оценки эффективности системы управления риском реализации информационных угроз.				

8.5 Направление 4 «Совершенствование системы управления риском реализации информационных угроз»

8.5.1 Процесс «Обеспечение соответствия фактических значений КПУР принятым»

8.5.1.1 Применяемые финансовой организацией меры по обеспечению соответствия фактических значений КПУР принятым должны обеспечивать:

- проведение анализа необходимости совершенствования системы управления риском реализации информационных угроз;
- принятие решений по совершенствованию системы управления риском реализации информационных угроз.

8.5.1.2 Состав мер по проведению анализа необходимости совершенствования системы управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 26.

Таблица 26 — Состав мер по проведению анализа необходимости совершенствования системы управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОСЗ.1	Проведение анализа эффективности системы в целях принятия решения о необходимости совершенствования системы управления риском реализации информационных угроз в следующих случаях:	—	—	—

Окончание таблицы 26

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОС3.1.1	- выявления фактов или возможности превышения сигнальных и контрольных значений КПУР	О	О	О
ОС3.1.2	- изменения политики финансовой организации в отношении принципов и приоритетов в реализации системы управления риском реализации информационных угроз	О	О	О
ОС3.1.3	- изменения политики финансовой организации в отношении величины допустимого риска реализации информационных угроз (риск-аппетита), сигнальных и контрольных значений КПУР	О	О	О
ОС3.1.4	- изменения политики финансовой организации в отношении аутсорсинга, в том числе в части взаимодействия с причастными сторонами — поставщиками услуг, включая поставщиков облачных услуг	О	О	О
ОС3.1.5	- внедрения финансовой организацией новых технологий предоставления финансовых и (или) информационных услуг, существенное изменение критичной архитектуры (в частности, бизнес- и технологических процессов)	О	О	О
ОС3.1.6	- изменения условий взаимодействия финансовой организации с причастными сторонами — поставщиками услуг, включая поставщиков облачных услуг	О	О	О
ОС3.1.7	- изменения законодательства Российской Федерации, в том числе нормативных актов Банка России	О	О	О
ОС3.2	Определение источников информации для проведения анализа необходимости совершенствования, включающих: - результаты оценки фактических значений КПУР и КИР; - результаты проведения самооценки и (или) профессиональной независимой оценки зрелости процессов обеспечения операционной надежности и защиты информации; - результаты проведенных сценарных анализов и тестирований готовности финансовой организации противостоять реализации информационных угроз (включая стресс-тестирования); - отчеты о выявленных событиях риска реализации информационных угроз; - отчеты о реагировании на инциденты и восстановлении после их реализации; - планы и решения по внедрению финансовой организацией новых технологий предоставления финансовых и (или) информационных услуг, - существенному изменению критичной архитектуры; - изменения в рамках пересмотра модели информационных угроз, предусмотренного мерой ВИО.16 настоящей таблицы; - результаты анализа эффективных практик в области обеспечения операционной надежности и защиты информации	О	О	О
ОС3.3	Фиксация и доведение до коллегиального исполнительного органа (а в случае его отсутствия — единоличного исполнительного органа) или подотчетных им коллегиальных органов финансовой организации и должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз, результатов (свидетельств) анализа эффективности такой системы в целях принятия решения о необходимости ее совершенствования	О	О	О

8.5.1.3 Состав мер по принятию решений по совершенствованию системы управления риском реализации информационных угроз применительно к уровням защиты приведен в таблице 27.

Таблица 27 — Состав мер по принятию решений по совершенствованию системы управления риском реализации информационных угроз

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОСЗ.4	Принятие коллегиальным исполнительным органом финансовой организации и должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз, решений по совершенствованию системы управления риском реализации информационных угроз на основе результатов проведения анализа необходимости совершенствования такой системы: - решение об отсутствии необходимости совершенствования такой системы; - решение о необходимости реализации тактических улучшений такой системы; - решение о необходимости инициирования реализации стратегических улучшений такой системы и доведение таких решений до совета директоров (наблюдательного совета) финансовой организации	О	О	О
ОСЗ.5	Рассмотрение и принятие решений о необходимости реализации стратегических улучшений системы управления риском реализации информационных угроз советом директоров (наблюдательным советом) финансовой организации	О	О	О
ОСЗ.6	Фиксация во внутренних документах финансовой организации принятых решений по совершенствованию системы управления риском реализации информационных угроз*	О	О	О
ОСЗ.7	Обеспечение со стороны должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз (с привлечением службы ИБ), контроля за реализацией тактических улучшений системы управления риском реализации информационных угроз	О	О	О
ОСЗ.8	Обеспечение со стороны коллегиального исполнительного органа финансовой организации и должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз (с привлечением службы ИБ), контроля за реализацией стратегических улучшений системы управления риском реализации информационных угроз	О	О	О
ОСЗ.9	Организация и выполнение деятельности по реализации тактических улучшений системы управления риском реализации информационных угроз, включая:	—	—	—
ОСЗ.9.1	- внедрение новых мер, пересмотр и исправление недостатков в применяемом составе организационных и технических мер по обеспечению операционной надежности и защиты информации	О	О	О
ОСЗ.9.2	- пересмотр и адаптацию способов выявления событий риска реализации информационных угроз в зависимости от модели информационных угроз	О	О	О
ОСЗ.10	Организация и выполнение деятельности по реализации стратегических улучшений системы управления риском реализации информационных угроз, включая:			

Окончание таблицы 27

Условное обозначение и номер меры	Содержание мер системы управления риском реализации информационных угроз	Уровень защиты		
		3	2	1
ОС3.10.1	- пересмотр политики управления риском реализации информационных угроз в части уточнения установленных в ней целей, состава и значений КПУР, а также пересмотр плана реагирования на риск реализации информационных угроз	О	О	О
ОС3.10.2	- пересмотр политики в отношении аутсорсинга, в том числе пересмотр соглашений об уровне оказания услуг (SLA)	О	О	О
ОС3.10.3	- пересмотр области применения системы управления риском реализации информационных угроз (критичной архитектуры)	О	О	О
ОС3.10.4	- пересмотр и доработку методологии оценки риска реализации информационных угроз	О	О	О
ОС3.10.5	- пересмотр объемов ресурсного обеспечения в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации	О	О	О
* В рамках фиксации решений по совершенствованию системы управления риском реализации информационных угроз должны быть приведены выводы об отсутствии необходимости тактических или стратегических улучшений системы либо указаны направления соответствующих улучшений.				

Приложение А
(обязательное)

Классификация событий риска реализации информационных угроз с точки зрения источников риска

А.1 Классификация событий риска реализации информационных угроз с точки зрения источников риска производится по четырем категориям:

- категория 1 «недостатки процессов»;
- категория 2 «действия персонала и других связанных с финансовой организацией лиц»;
- категория 3 «сбои объектов информатизации»[1)];
- категория 4 «внешние факторы».

А.2 Финансовая организация классифицирует события риска реализации информационных угроз с точки зрения источников риска первого уровня по четырем категориям согласно А.1, а также по уязвимостям, обусловленным недостатками процессов обеспечения операционной надежности и защиты информации, посредством которых реализована информационная угроза.

А.3 В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «недостатки процессов» относит:

- недостатки процессов применения технологических мер защиты информации, обрабатываемой в рамках технологических операций при выполнении бизнес- и технологических процессов;
- недостатки процессов применения прикладного программного обеспечения автоматизированных систем и приложений, соответствующих требованиям к обеспечению защиты информации [8]—[10];
- недостатки процессов планирования, реализации, контроля и совершенствования процессов обеспечения операционной надежности и защиты информации;
- недостатки других внутренних процессов, связанных с обеспечением операционной надежности и защиты информации финансовой организации.

А.4 В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «действия персонала и других связанных с финансовой организацией лиц» относит реализацию несанкционированного доступа работников финансовой организации или третьих лиц, обладающих полномочиями доступа к объектам информатизации инфраструктурного уровня финансовой организации (действия внутреннего нарушителя).

А.5 В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «сбои объектов информатизации» относит сбои и отказы в работе объектов информатизации в результате реализации информационных угроз.

А.6 В целях дополнительной классификации событий риска реализации информационных угроз финансовая организация к категории «внешние факторы» относит реализацию компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информатизации инфраструктурного уровня финансовой организации (действия внешнего нарушителя), в том числе с целью:

- блокирования штатного функционирования бизнес- и технологических процессов финансовой организации;
- хищения, искажения, удаления информации конфиденциального характера (включая персональные данные).

А.7 В рамках дополнительной детализации классификации источников риска реализации информационных угроз финансовые организации классифицируют источники риска с точки зрения направлений компьютерных атак, типов компьютерных атак и компьютерных инцидентов и типов атакуемых объектов.

А.7.1 По вектору (направлению) компьютерных атак:

- компьютерные атаки, направленные на объекты информатизации финансовой организации;
- компьютерные атаки, направленные на клиента финансовой организации.

А.7.2 По типам компьютерных атак и компьютерных инцидентов, определяемых согласно форматам представления информации о компьютерных инцидентах в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, учитывающим формы и сроки взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов [32].

А.7.3 По типам атакуемых объектов:

а) на инфраструктурном уровне объектов информатизации (системном уровне информационной инфраструктуры):

[1)] Отказы и (или) нарушения функционирования применяемых финансовой организацией объектов информатизации и (или) несоответствие их функциональных возможностей и характеристик потребностям финансовой организации.

- аппаратное обеспечение;
- сетевое оборудование;
- сетевые приложения и сервисы;
- серверные компоненты виртуализации, программные инфраструктурные сервисы;
- операционные системы, системы управления базами данных, сервера приложений;

б) на прикладном уровне объектов информатизации (уровне автоматизированных систем и приложений), используемых для выполнения бизнес- и технологических процессов финансовой организации при оказании финансовых и (или) информационных 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;
- автоматизированные системы, используемые работниками финансовой организации;

в) на прикладном уровне объектов информатизации (уровне автоматизированных систем и приложений), используемых клиентом финансовой организации при получении финансовых и (или) информационных услуг:

- мобильное приложение;
- файловый сервер;
- система дистанционного банковского обслуживания;
- сервер электронной почты;
- автоматизированная система, используемая работниками клиента финансовой организации;

г) другой тип объектов информатизации;

д) работники финансовой организации;

е) причастные стороны финансовой организации (за исключением клиентов финансовой организации);

ж) клиенты финансовой организации.

Приложение Б
(обязательное)

Классификация событий риска реализации информационных угроз и событий операционной надежности с точки зрения типов событий реализации информационных угроз

Б.1 Финансовая организация дополнительно классифицирует риск реализации информационных угроз по событиям риска в разрезе следующих типов событий реализации информационных угроз.

Примечание — Кредитные организации при классификации события риска реализации информационных угроз с точки зрения типов событий применяют в качестве первого уровня классификации типы событий операционной риска, установленные нормативными актами Банка России [6]:

преднамеренные действия персонала;
преднамеренные действия третьих лиц;
нарушение кадровой политики и безопасности труда;
нарушение прав клиентов и контрагентов;
ущерб материальным активам;
нарушение и сбои систем и оборудования;
нарушение организации, исполнения и управления процессами.

Б.1.1 События реализации информационных угроз, связанные с осуществлением операций по переводу денежных средств без согласия клиентов.

Б.1.2 События реализации информационных угроз, связанные с осуществлением финансовых сделок с использованием финансовой платформы без волеизъявления участников финансовой платформы.

Б.1.3 События реализации информационных угроз, связанные с осуществлением несанкционированных финансовых (банковских) операций[1)].

Б.1.4 События реализации информационных угроз, связанные с нарушением операционной надежности.

Б.1.5 События реализации информационных угроз, связанные с выявлением уязвимостей в объектах информатизации финансовой организации.

Б.1.6 События реализации информационных угроз, связанные с неконтролируемым распространением информации конфиденциального характера (утечками информации).

Б.1.7 События реализации информационных угроз, связанные с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры и приводящие к утечке, искажению или потере информации конфиденциального характера (включая персональные данные), а также к случаям побуждения клиентов финансовой организации к осуществлению финансовых (банковских) операций, в том числе операций по переводу денежных средств путем обмана или злоупотребления доверием (методов социальной инженерии), которые привели и (или) могут привести к случаям мошенничества и (или) кражи с банковского счета в отношении клиентов финансовой организации.

Б.2 Детализация классификации по событиям реализации информационных угроз, связанных с возникновением финансовых инцидентов, приведена в таблицах Б.1—Б.18.

[1)] За исключением событий реализации информационных угроз, определенных в Б.1.1 и Б.1.2.

Таблица Б.1 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для кредитных организаций

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады	—	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период: более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более; более четырех часов для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; более шести часов для банка с БЛ
Бизнес- и технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады	—	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период: более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более; более четырех часов для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; более шести часов для банка с БЛ и НКО
Бизнес- и технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет	Событие, связанное с размещением привлеченных во вклады денежных средств клиентов — физических и (или) юридических лиц от своего имени и за свой счет в результате НСД к объектам информатизации кредитной организации	Событие, связанное с простоем или деградацией бизнес- и технологического процесса: на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более; на период более четырех часов для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; на период более шести часов для банка с БЛ и НКО
Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам	Событие, связанное с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента — физического лица ОПДС	Событие, связанное с простоем или деградацией бизнес- и технологического процесса: на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более на период более четырех часов* для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; на период более шести часов* для банка с БЛ
	Событие, связанное с осуществлением перевода денежных средств по поручению клиента — физических лиц с искаженными реквизитами в результате НСД к объектам информатизации ОПДС	
Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их	Событие, связанное с осуществлением перевода денежных средств на основании несанкционированно модифицированного распоряжения клиента — юридического лица ОПДС, в том числе банка-корреспондента,	Событие, связанное с простоем или деградацией бизнес- и технологического процесса: на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более;

Продолжение таблицы Б.1

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
банковским счетам, за исключением переводов по распоряжениям участников платежной системы	за исключением переводов по распоряжениям участников платежной системы	на период более четырех часов* для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; на период более шести часов* для банка с БЛ и НКО
	Событие, связанное с осуществлением перевода денежных средств по поручению клиента — юридических лиц, в том числе банков-корреспондентов с искаженными реквизитами в результате НСД к объектам информатизации ОПДС	
Бизнес- и технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц	Событие, связанное с изменением остатка на банковском счете клиента — физического лица в результате НСД к объектам информатизации кредитной организации	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ
Бизнес- и технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц	Событие, связанное с изменением остатка на банковском счете клиента — юридического лица в результате НСД к объектам информатизации кредитной организации	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ и НКО
Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов)	Событие, связанное с осуществлением перевода денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), на основании несанкционированно модифицированного распоряжения клиента оператора по переводу денежных средств	Событие, связанное с простоем или деградацией бизнес- и технологического процесса: на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более; на период более четырех часов* для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей; на период более шести часов* для банка с БЛ и НКО
	Событие, связанное с осуществлением перевода денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов), с искаженными реквизитами в результате НСД к объектам информатизации ОПДС	
Бизнес- и технологический процесс, обеспечивающий выполнение операций на финансовых рынках	—	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более 24 часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ

Окончание таблицы Б.1

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий выполнение кассовых операций	Событие, связанное с несанкционированной выдачей наличных денежных средств кредитной организацией	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ
	Событие, связанное с несанкционированным зачислением денежных средств	
Бизнес- и технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций	—	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ
Бизнес- и технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе	Событие, связанное с нарушением целостности (подмены, удаления) или нарушением достоверности (внесения фиктивных биометрических персональных данных) биометрических персональных данных	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ
Бизнес- и технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	Событие, связанное с ложно-положительной идентификацией и (или) аутентификацией с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия	Событие, связанное с простоем или деградацией бизнес- и технологического процесса на период более двух часов для банка, размер активов которого составляет 500 миллиардов рублей и более, для банка с УЛ, размер активов которого составляет менее 500 миллиардов рублей, банка с БЛ
	Событие, связанное с идентификацией и (или) аутентификацией с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия, при подмене физическим лицом биометрических персональных данных	

* Для кредитных организаций, признанных значимыми на рынке платежных услуг в соответствии с нормативным актом Банка России [3], пороговый уровень допустимого времени простоя и (или) деградации технологических процессов составляет два часа.

Таблица Б.2 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих брокерскую деятельность

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств	Событие, связанное с возвратом денежных средств на основании требования клиента брокера, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
	Событие, связанное с возвратом денежных средств в результате НСД к объектам информатизации брокера или объектам информатизации взаимодействия брокера и кредитной организации	
Бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет	Событие, связанное с внесением записей во внутренний учет в результате НСД к объектам информатизации брокера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 12 часов
Бизнес- и технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами	Событие, связанное с исполнением поручения клиента на совершение сделки, сформированного без его согласия, в том числе на основании модифицированного поручения клиента	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более четырех часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с исполнением поручения клиента на совершение сделки в результате НСД к объектам информатизации брокера или объектам информатизации взаимодействия брокера и организатора торговли	

Таблица Б.3 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих дилерскую деятельность

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий совершение сделок купли-продажи ценных бумаг от своего имени и за свой счет путем публичного объявления цен покупки и (или) продажи определенных ценных бумаг с обязательством покупки и (или) продажи этих ценных бумаг по объявленным лицом, осуществляющим указанную деятельность, ценам	Событие, связанное с совершением сделки купли-продажи ценных бумаг в результате НСД к объектам информатизации дилера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
Бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет	Событие, связанное с внесением записей во внутренний учет в результате НСД к объектам информатизации дилера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 12 часов

Таблица Б.4 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, для некредитных финансовых организаций, осуществляющих деятельность форекс-дилера

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет	Событие, связанное с внесением записей во внутренний учет в результате НСД к объектам информатизации форекс-дилера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 12 часов
Бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств	Событие, связанное с возвратом клиенту денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
	Событие, связанное с возвратом клиентам денежных средств в результате НСД к инфраструктуре форекс-дилера или инфраструктуре взаимодействия форекс-дилера и кредитной организации	
Бизнес- и технологический процесс, обеспечивающий заключение от своего имени и за свой счет с физическими лицами, не являющимися индивидуальными предпринимателями, не на организованных торгах договоров, указанных в пункте 4.1 [33]	Событие, связанное с заключением от своего имени и за свой счет договора в результате НСД к объектам информатизации форекс-дилера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов

Таблица Б.5 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность по управлению ценными бумагами

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет	Событие, связанное с внесением записей во внутренний учет в результате НСД к объектам информатизации управляющего ценными бумагами	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 12 часов
Бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств	Событие, связанное с возвратом клиенту денежных средств на основании требования клиента, сформированного без его согласия, в том числе на основании модифицированного требования клиента	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
	Событие, связанное с возвратом клиенту денежных средств в результате НСД к инфраструктуре управляющего или инфраструктуре взаимодействия управляющего и кредитной организации	
Бизнес- и технологический процесс, обеспечивающий совершение сделок с ценными бумагами и (или) заключение договоров, являющихся производными финансовыми инструментами в интересах учредителя управления	Событие, связанное с совершением сделки с ценными бумагами и (или) заключением договора, являющегося производным финансовым инструментом, в результате НСД к объектам информатизации дилера	Событие, связанное с простоем и (или) деградацией технологического процесса на период более четырех часов

Таблица Б.6 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность регистратора

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг	Событие, связанное с внесением учетных записей в реестр владельцев ценных бумаг в результате НСД к объектам информатизации регистратора	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
Бизнес- и технологический процесс, обеспечивающий осуществление регистратором сверки учитываемых регистратором прав на ценные бумаги с центральным депозитарием по счету номинального держателя центрального депозитария	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более четырех часов

Таблица Б.7 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих депозитарную деятельность, включая деятельность центрального депозитария

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий внесение учетных записей в учетные регистры	Событие, связанное с внесением учетных записей в учетные регистры в результате НСД к объектам информатизации регистратора	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
Бизнес- и технологический процесс, обеспечивающий выплату депоненту доходов в денежной форме по ценным бумагам, учет прав на которые осуществляет депозитарий, и иных причитающихся владельцам указанных ценных бумаг денежных выплат	Событие, связанное с выплатой депоненту доходов в денежной форме по ценным бумагам в результате НСД к объектам информатизации депозитария или объектам информатизации взаимодействия депозитария и кредитной организации	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
Бизнес- и технологический процесс, обеспечивающий осуществление расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах	Событие, связанное с осуществлением расчетов по результатам сделок, совершенных на организованных торгах, на основании модифицированного поручения о движении ценных бумаг, направленного клиринговой организацией	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов
	Событие, связанное с осуществлением расчетов по результатам сделок, совершенных на организованных торгах, в результате НСД к объектам информатизации расчетного депозитария	
Бизнес- и технологический процесс, обеспечивающий осуществление центральным депозитарием сверки учитываемых центральным депозитарием прав на ценные бумаги с регистратором по счету номинального держателя центрального депозитария	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более четырех часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]

Таблица Б.8 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность организатора торговли

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий раскрытие и предоставление информации организатором торговли	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий ведение реестра участников торгов и их клиентов, реестра заявок, реестр заключенных на организованных торгах договоров, реестра внебиржевых договоров	Событие, связанное с внесением изменений в реестр участников торгов и их клиентов, реестр заявок, реестр заключенных на организованных торгах договоров, реестр внебиржевых договоров в результате НСД к инфраструктуре организатора торговли	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий заключение договора между участниками торгов	Событие, связанное с заключением договора между участниками торгов на основании заявки участника торгов, сформированной без его согласия, в том числе на основании модифицированной заявки участника торгов	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с заключением договора между участниками торгов или формированием реестра договоров в результате НСД к объектам информатизации организатора торговли	

Таблица Б.9 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих клиринговую деятельность и деятельность центрального контрагента

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий определение подлежащих исполнению обязательств	Событие, связанное с определением подлежащих исполнению обязательств на основании модифицированного реестра договоров, направленного организатором торговли	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с определением подлежащих исполнению обязательств в результате НСД к объектам информатизации клиринговой организации	
Бизнес- и технологический процесс, обеспечивающий направление поручения на возврат имущества, являющегося клиринговым обеспечением	Событие, связанное с направлением поручения на возврат имущества, являющегося клиринговым обеспечением, на основании поручения участника клиринга, сформированного без его согласия, в том числе на основании модифицированного поручения	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с направлением поручения на возврат имущества, являющегося клиринговым обеспечением, в результате НСД к объектам информатизации клиринговой организации или объектам информатизации взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	
Бизнес- и технологический процесс, обеспечивающий совершение действий, направленных на исполнение подлежащих исполнению обязательств	Событие, связанное с совершением действий, направленных на исполнение подлежащих исполнению обязательств, на основании модифицированного реестра договоров, направленного организатором торговли	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с совершением действий, направленных на исполнение подлежащих исполнению обязательств, на основании реестра договоров, в результате НСД к объектам информатизации клиринговой организации или объектам информатизации взаимодействия клиринговой организации и расчетной организации, расчетного депозитария	

Таблица Б.10 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих репозитарную деятельность

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий учет заключенных не на организованных торгах договоров РЕПО, договоров, являющихся производными финансовыми инструментами, а также иных договоров	Событие, связанное с учетом заключенного не на организованных торгах договоров РЕПО, договора, являющегося производным финансовым инструментом или иного договора, на основании электронного сообщения клиента репозитария, сформированного без его согласия, в том числе на основании модифицированного электронного сообщения клиента репозитария	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 12 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с учетом заключенного не на организованных торгах договоров РЕПО, договора, являющегося производным финансовым инструментом или иного договора, в результате НСД к объектам информатизации репозитария	
Бизнес- и технологический процесс, обеспечивающий учет регистратором финансовых транзакций информации о совершении финансовых сделок и об операциях по ним с использованием финансовой платформы	Событие, связанное с учетом совершенных финансовых сделок и операций по ним с использованием финансовой платформы на основании электронного сообщения оператора финансовой платформы, сформированного без его согласия или на основании модифицированного электронного сообщения оператора финансовой платформы	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с учетом совершенных финансовых сделок и операций по ним с использованием финансовой платформы в результате НСД к объектам информатизации регистратора финансовых транзакций или объектам информатизации взаимодействия оператора финансовой платформы и регистратора финансовых транзакций	
Бизнес- и технологический процесс, обеспечивающий передачу (предоставление) реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более шести часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]

Таблица Б.11 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий доверительное управление имуществом фондов, в том числе осуществление прав, удостоверенных ценными бумагами, составляющими фонды	Событие, связанное с осуществлением операций с имуществом фондов в результате НСД к объектам информатизации управляющей компании	Событие, связанное с простоем и (или) деградацией технологического процесса на период более двух часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий осуществление учета имущества фондов и контроля за распоряжением им, в том числе процесс взаимодействия со специализированным депозитарием	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий реализацию прав владельцев инвестиционных паев	Событие, связанное с изменением прав владельцев инвестиционных паев в реестре владельцев инвестиционных паев в результате НСД к объектам информатизации управляющей компании	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с погашением инвестиционного пая на основании электронного сообщения владельца инвестиционного пая, сформированного без его согласия или на основании модифицированного электронного сообщения владельца инвестиционного пая	
	Событие, связанное с погашением инвестиционного пая в результате НСД к объектам информатизации управляющей компании	
	Событие, связанное с выплатой денежной компенсации при прекращении договора доверительного управления фондом в результате НСД к объектам информатизации управляющей компании	

Таблица Б.12 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий осуществление специализированным депозитарием контроля за распоряжением имуществом клиентов	Событие, связанное с согласованием нелегитимных заявок, направленных из скомпрометированных объектов информатизации управляющей компании и (или) фондов	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
Бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг (в случае оказания услуг по ведению реестра владельцев инвестиционных паев паевых инвестиционных фондов, ипотечных сертификатов участия)	Событие, связанное с внесением учетных записей в реестр владельцев ценных бумаг в результате НСД к инфраструктуре регистратора	

Таблица Б.13 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность негосударственных пенсионных фондов

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий осуществление выплат вкладчикам, участникам, застрахованным лицам и их правопреемникам негосударственного пенсионного фонда в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения	Событие, связанное с осуществлением выплат в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения в результате НСД к объектам информатизации негосударственного пенсионного фонда или объектам информатизации взаимодействия негосударственного пенсионного фонда и кредитной организации	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий размещение средств пенсионных резервов	Событие, связанное с размещением средств пенсионных резервов в результате НСД к объектам информатизации негосударственного пенсионного фонда или объектам информатизации взаимодействия негосударственного пенсионного фонда и кредитной организации	

Окончание таблицы Б.13

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий передачу средств пенсионных резервов и пенсионных накоплений управляющей компании	Событие, связанное с передачей средств пенсионных резервов и пенсионных накоплений управляющей компании в результате НСД к объектам информатизации негосударственного пенсионного фонда или объектам информатизации взаимодействия негосударственного пенсионного фонда и кредитной организации	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий перевод выкупных сумм (средств пенсионных накоплений) в иные негосударственные пенсионные фонды и Пенсионный фонд Российской Федерации	Событие, связанное с переводом выкупных сумм в результате НСД к объектам информатизации негосударственного пенсионного фонда или объектам информатизации взаимодействия негосударственного пенсионного фонда и кредитной организации	
Бизнес- и технологический процесс, обеспечивающий расторжение договора негосударственного пенсионного обеспечения, договора об обязательном пенсионном страховании с негосударственным пенсионным фондом	Событие, связанное с осуществлением выплат в связи с расторжением договора на основании заявления клиента негосударственного пенсионного фонда, сформированного без его согласия, в том числе на основании модифицированного заявления	
	Событие, связанное с осуществлением выплат в связи с расторжением договора в результате НСД к объектам информатизации негосударственного пенсионного фонда или объектам информатизации взаимодействия негосударственного пенсионного фонда и кредитной организации	

Таблица Б.14 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность субъектов страхового дела

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий учет страховых случаев	Событие, связанное с выплатой возмещения на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
	Событие, связанное с выплатой возмещения в результате НСД к инфраструктуре субъектов страхового дела	
Бизнес- и технологический процесс, обеспечивающий работу сайтов в части размещения информации, предусмотренной пунктом 6 статьи 6 Закона Российской Федерации [34]	—	
Бизнес- и технологический процесс, обеспечивающий возврат страховой премии	Событие, связанное с возвратом страховой премии на основании заявления клиента, сформированного без его согласия, в том числе на основании модифицированного заявления	
	Событие, связанное с возвратом страховой премии в результате НСД к объектам информатизации субъектов страхового дела	

Таблица Б.15 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность операторов инвестиционных платформ

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий предоставление доступа к инвестиционной платформе	—	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий размещение инвестиционного предложения	Событие, связанное с размещением инвестиционного предложения на основании поручения лица, привлекающего инвестиции, сформированного без его согласия, в том числе на основании модифицированного поручения лица, привлекающего инвестиции	
	Событие, связанное с размещением инвестиционного предложения в результате НСД к объектам информатизации оператора инвестиционной платформы	

Продолжение таблицы Б.15

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем предоставления займов	Событие, связанное с заключением договора инвестирования путем предоставления займов на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с заключением договора инвестирования путем предоставления займов без согласия инвестора в результате НСД к объектам информатизации оператора инвестиционной платформы	
	Событие, связанное с заключением договора инвестирования путем предоставления займов без согласия лица, привлекающего инвестиции, в результате НСД к объектам информатизации оператора инвестиционной платформы	
Бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы	Событие, связанное с заключением договора инвестирования путем приобретения эмиссионных ценных бумаг на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	
	Событие, связанное с заключением договора инвестирования путем приобретения эмиссионных ценных бумаг без согласия инвестора в результате НСД к объектам информатизации оператора инвестиционной платформы	
	Событие, связанное с заключением договора инвестирования путем приобретения эмиссионных ценных бумаг без согласия лица, привлекающего инвестиции, в результате НСД к объектам информатизации оператора инвестиционной платформы	
Бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав	Событие, связанное с заключением договора инвестирования путем приобретения утилитарных цифровых прав на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	

Окончание таблицы Б.15

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав	Событие, связанное с заключением договора инвестирования путем приобретения утилитарных цифровых прав без согласия инвестора в результате НСД к объектам информатизации оператора инвестиционной платформы	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с заключением договора инвестирования путем приобретения утилитарных цифровых прав без согласия лица, привлекающего инвестиции, в результате НСД к объектам информатизации оператора инвестиционной платформы	
	Событие, связанное с возникновением, распоряжением или передачей утилитарных цифровых прав в результате НСД к объектам информатизации оператора инвестиционной платформы	
Бизнес- и технологический процесс, обеспечивающий инвестирование путем приобретения цифровых финансовых активов	Событие, связанное с заключением договора инвестирования путем приобретения цифровых финансовых активов на основании заявки инвестора, сформированной без его согласия, в том числе на основании модифицированной заявки инвестора	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с заключением договора инвестирования путем приобретения цифровых финансовых активов без согласия инвестора в результате НСД к объектам информатизации оператора инвестиционной платформы	
	Событие, связанное с заключением договора инвестирования путем приобретения цифровых финансовых активов без согласия лица, привлекающего инвестиции, в результате НСД к объектам информатизации оператора инвестиционной платформы	
Бизнес- и технологический процесс, обеспечивающий инвестирование путем приобретения цифровых финансовых активов	Событие, связанное с возникновением, распоряжением или передачей цифровых финансовых активов в результате НСД к объектам информатизации оператора инвестиционной платформы	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]

Таблица Б.16 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность операторов финансовых платформ

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы	Событие, связанное с переводом активов потребителя финансовых услуг со специального счета на основании требования потребителя финансовых услуг, сформированного без его согласия, в том числе на основании модифицированного требования потребителя финансовых услуг	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более четырех часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с переводом активов потребителя финансовых услуг со специального счета в результате НСД к объектам информатизации оператора финансовой платформы	
	Событие, связанное с совершением финансовых сделок на основании заявки потребителя финансовых услуг, сформированной без его согласия, в том числе на основании модифицированной заявки потребителя финансовых услуг	
	Событие, связанное с совершением финансовых сделок в результате НСД к объектам информатизации оператора финансовой платформы или объектам информатизации взаимодействия потребителя финансовых услуг и финансовой платформы	

Таблица Б.17 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий выпуск цифровых финансовых активов в информационной системе	Событие, связанное с выпуском цифровых финансовых активов на основании запроса о выпуске цифровых финансовых активов, сформированного без согласия лица, выпускающего цифровые финансовые активы, в том числе на основании модифицированного запроса	Событие, связанное с простоем и (или) деградацией технологического процесса на период более 24 часов
	Событие, связанное с выпуском цифровых финансовых активов в результате НСД к объектам информатизации оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов	
	Событие, связанное с выпуском цифровых финансовых активов в результате эксплуатации недостатков (уязвимостей) алгоритма (алгоритмов), обеспечивающего тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	
Бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев акций непубличных акционерных обществ, осуществляющих выпуск цифровых финансовых активов, удостоверяющих права участия в капитале указанных непубличных акционерных обществ	Событие, связанное с внесением учетных записей в реестр владельцев акций непубличных акционерных обществ, осуществляющих выпуск цифровых финансовых активов, удостоверяющих права участия в капитале указанных непубличных акционерных обществ, в результате НСД к объектам информатизации оператора информационных систем, в которой осуществляется выпуск цифровых финансовых активов	

Продолжение таблицы Б.17

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий внесение записей оператором информационной системы в соответствии с частью 2 статьи 6 Федерального закона [35]	Событие, связанное с внесением записей в реестр оператора информационных систем, в которых осуществляется выпуск цифровых финансовых активов, в результате НСД к объектам информатизации оператора	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более двух часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более четырех часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий доступ к информационной системе, в том числе ведение реестра пользователей информационной системы	—	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более шести часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более 12 часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий взаимодействие с оператором обмена цифровых финансовых активов	—	
Бизнес- и технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе погашение записей о цифровых финансовых активах	Событие, связанное с обращением цифровых финансовых активов на основании запроса об обращении цифровых финансовых активов, сформированного без согласия владельца цифровых финансовых активов, в том числе на основании модифицированного запроса	
	Событие, связанное с обращением цифровых финансовых активов в результате НСД к объектам информатизации оператора информационной системы, в которой осуществляется выпуск цифровых финансовых активов	

Окончание таблицы Б.17

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе погашение записей о цифровых финансовых активах	Событие, связанное с обращением цифровых финансовых активов в результате эксплуатации недостатков (уязвимостей) алгоритма (алгоритмов), обеспечивающего (обеспечивающих) тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр (алгоритмы консенсуса)	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более шести часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более 12 часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
Бизнес- и технологический процесс, обеспечивающий мониторинг тождественности информации, содержащейся во всех базах данных, составляющих распределенный реестр	—	

Таблица Б.18 — Детализированная классификация событий реализации информационных угроз, связанных с осуществлением несанкционированных финансовых (банковских) операций, а также событий реализации информационных угроз, связанных с нарушением операционной надежности, для некредитных финансовых организаций, осуществляющих деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
Бизнес- и технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами	Событие, связанное с совершением сделок с цифровыми финансовыми активами на основании запроса на обмен цифровых финансовых активов, сформированного без согласия лица, обменивающего цифровые финансовые активы, в том числе на основании модифицированного запроса	Событие, связанное с простоем и (или) деградацией технологического процесса: на период более шести часов для некредитной финансовой организации, обязанной соблюдать усиленный или стандартный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]; на период более 12 часов для некредитной финансовой организации, обязанной соблюдать минимальный уровень защиты информации в соответствии с требованиями нормативных актов Банка России [9]
	Событие, связанное с передачей цифровых финансовых активов на цифровой кошелек, отличный от цифрового кошелька получателя цифровых финансовых активов, в результате НСД к объектам информатизации оператора обмена цифровых финансовых активов	

Окончание таблицы Б.18

Бизнес- и технологический процесс	Событие реализации информационных угроз, связанное с осуществлением несанкционированных финансовых (банковских) операций	Событие реализации информационных угроз, связанное с нарушением операционной надежности
	Событие, связанное с совершением сделок с цифровыми финансовыми активами в результате эксплуатации недостатков (уязвимостей) алгоритма (алгоритмов), обеспечивающего тождественность информации, содержащейся во всех базах данных, составляющих распределенный реестр	
	Событие, связанное с совершением сделок с цифровыми финансовыми активами в результате НСД к объектам информатизации оператора обмена цифровых финансовых активов или объектам информатизации взаимодействия лица, обменивающего цифровые финансовые активы, и информационной системы, в которой осуществляется обмен цифровых финансовых активов	
Бизнес- и технологический процесс, обеспечивающий взаимодействие с оператором информационной системы	—	

Приложение В
(обязательное)

Классификация событий риска реализации информационных угроз в разрезе видов (направлений) деятельности финансовых организаций

В.1 Классификация событий риска реализации информационных угроз с точки зрения видов (направлений) деятельности осуществляется финансовой организацией согласно подходу, описанному ниже.

В.2 Кредитные организации классифицируют события риска реализации информационных угроз с точки зрения следующих видов (направлений) деятельности первого уровня [6], представленных в В.2.1—В.2.9.

В.2.1 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).

В.2.2 Осуществление операций и сделок с финансовыми инструментами торгового портфеля (операции и сделки на финансовом рынке).

В.2.3 Оказание банковских услуг розничным клиентам, кроме брокерских и депозитарных услуг (розничное банковское обслуживание).

В.2.4 Оказание юридическим лицам банковских услуг, за исключением основного вида (направления) деятельности первого уровня кредитной организации, указанного в В.2.1 (коммерческое банковское обслуживание корпоративных клиентов).

В.2.5 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 кредитной организации, указанным в В.2.3, В.2.4, В.2.6—В.2.8 (осуществление переводов денежных средств, платежей и расчетов через платежные системы).

В.2.6 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 услуги и депозитарные услуги).

В.2.7 Управление активами клиентов по договорам доверительного управления (управление активами).

В.2.8 Брокерское обслуживание розничных клиентов (розничное брокерское обслуживание).

В.2.9 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).

В.3 В качестве последующего уровня классификации события риска реализации информационных угроз классифицируются кредитными организациями по направлениям деятельности с точки зрения следующих бизнес- и технологических процессов, представленных в В.3.1—В.3.13.

В.3.1 Бизнес- и технологический процесс, обеспечивающий привлечение денежных средств физических лиц во вклады.

В.3.2 Бизнес- и технологический процесс, обеспечивающий привлечение денежных средств юридических лиц во вклады.

В.3.3 Бизнес- и технологический процесс, обеспечивающий размещение привлеченных во вклады денежных средств физических и (или) юридических лиц от своего имени и за свой счет.

В.3.4 Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению физических лиц по их банковским счетам.

В.3.5 Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств по поручению юридических лиц, в том числе банков-корреспондентов, по их банковским счетам, за исключением переводов по распоряжениям участников платежной системы[1)].

В.3.6 Бизнес- и технологический процесс, обеспечивающий открытие и ведение банковских счетов физических лиц.

В.3.7 Бизнес- и технологический процесс, обеспечивающий открытие и ведение банковских счетов юридических лиц.

В.3.8 Бизнес- и технологический процесс, обеспечивающий осуществление переводов денежных средств без открытия банковских счетов, в том числе электронных денежных средств (за исключением почтовых переводов).

[1)] В случае переводов по распоряжениям участников платежной системы показатель устанавливается в соответствии с нормативным актом Банка России [36].

В.3.9 Бизнес- и технологический процесс, обеспечивающий выполнение операций на финансовых рынках.

В.3.10 Бизнес- и технологический процесс, обеспечивающий выполнение кассовых операций.

В.3.11 Бизнес- и технологический процесс, обеспечивающий работу онлайн-сервисов дистанционного обслуживания и доступа к осуществлению операций.

В.3.12 Бизнес- и технологический процесс, обеспечивающий размещение и обновление биометрических персональных данных в единой биометрической системе.

В.3.13 Бизнес- и технологический процесс, обеспечивающий идентификацию и (или) аутентификацию с использованием биометрических персональных данных физических лиц, в том числе с применением информационных технологий без их личного присутствия.

В.4 Некредитные финансовые организации классифицируют события риска реализации информационных угроз с точки зрения следующих видов (направлений) деятельности первого уровня, представленных в В.4.1—В.4.16.

В.4.1 Осуществление деятельности профессиональных участников рынка ценных бумаг:

- осуществление брокерской деятельности;
- осуществление дилерской деятельности;
- осуществление деятельности по управлению ценными бумагами;
- осуществление деятельности регистратора;
- осуществление депозитарной деятельности, включая деятельность центрального депозитария.

В.4.2 Осуществление деятельности управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда.

В.4.3 Осуществление деятельности специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда.

В.4.4 Осуществление клиринговой деятельности и деятельности центрального контрагента.

В.4.5 Осуществление деятельности организатора торговли.

В.4.6 Осуществление репозитарной деятельности.

В.4.7 осуществление деятельности регистратора финансовых транзакций.

В.4.8 Осуществление деятельности субъектов страхового дела.

В.4.9 Осуществление деятельности негосударственных пенсионных фондов.

В.4.10 Осуществление деятельности микрофинансовых организаций.

В.4.11 Осуществление деятельности кредитных потребительских кооперативов.

В.4.12 Осуществление деятельности жилищных накопительных кооперативов.

В.4.13 Осуществление деятельности сельскохозяйственных кредитных потребительских кооперативов.

В.4.14 Осуществление деятельности оператора инвестиционной платформы.

В.4.15 Осуществление деятельности ломбардов.

В.4.16 Осуществление деятельности оператора финансовой платформы.

В.4.17 Осуществление деятельности операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов.

В.4.18 Осуществление деятельности операторов обмена цифровых финансовых активов.

В.5 В рамках дополнительной детализации классификации событий риска реализации информационных угроз с точки зрения видов (направлений) деятельности отдельные некредитные финансовые организации классифицируют виды (направления) деятельности, в том числе с точки зрения составляющих их бизнес- и технологических процессов, представленных в В.5.1—В.5.17.

В.5.1 Осуществление брокерской деятельности:

- бизнес- и технологический процесс, обеспечивающий исполнение поручений клиентов на совершение сделок с ценными бумагами и заключение договоров, являющихся производными финансовыми инструментами;
- бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет;
- бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств.

В.5.2 Осуществление дилерской деятельности:

- бизнес- и технологический процесс, обеспечивающий совершение сделок купли-продажи ценных бумаг от своего имени и за свой счет путем публичного объявления цен покупки и (или) продажи определенных ценных бумаг с обязательством покупки и (или) продажи этих ценных бумаг по объявленным лицом, осуществляющим такую деятельность, ценам;
- бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет.

В.5.3 Осуществление деятельности форекс-дилера:

- бизнес- и технологический процесс, обеспечивающий заключение от своего имени и за свой счет с физическими лицами, не являющимися индивидуальными предпринимателями, не на организованных торгах сделок, перечисленных в ст. 4.1 Федерального закона [33];
- бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет;
- бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств.

В.5.4 Осуществление деятельности по управлению ценными бумагами:

- бизнес- и технологический процесс, обеспечивающий совершения сделок с ценными бумагами и (или) заключения договоров, являющихся производными финансовыми инструментами в интересах учредителя управления;
- бизнес- и технологический процесс, обеспечивающий внесение записей во внутренний учет;
- бизнес- и технологический процесс, обеспечивающий возврат клиентам денежных средств.

В.5.5 Осуществление деятельности регистратора:

- бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг;
- бизнес- и технологический процесс, обеспечивающий осуществление регистратором сверки учитываемых регистратором прав на ценные бумаги с центральным депозитарием по счету номинального держателя центрального депозитария.

В.5.6 Осуществление депозитарной деятельности, включая деятельность центрального депозитария:

- бизнес- и технологический процесс, обеспечивающий внесение учетных записей в учетные регистры;
- бизнес- и технологический процесс, обеспечивающий осуществление расчетным депозитарием расчетов по результатам сделок, совершенных на организованных торгах;
- бизнес- и технологический процесс, обеспечивающий выплату депоненту доходов в денежной форме, причитающихся владельцам ценных бумаг;
- бизнес- и технологический процесс, обеспечивающий осуществление центральным депозитарием сверки учитываемых центральным депозитарием прав на ценные бумаги с регистратором по счету номинального держателя центрального депозитария.

В.5.7 Осуществление деятельности управляющих компаний инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда:

- бизнес- и технологический процесс, обеспечивающий доверительное управление имуществом фондов, в том числе осуществление прав, удостоверенных ценными бумагами, составляющими фонды;
- бизнес- и технологический процесс, обеспечивающий реализацию прав владельцев инвестиционных паев;
- бизнес- и технологический процесс, обеспечивающий осуществление учета имущества фондов и контроля за его распоряжением им, в том числе процесс взаимодействия со специализированным депозитарием.

В.5.8 Осуществление деятельности специализированных депозитариев инвестиционного фонда, паевого инвестиционного фонда и негосударственного пенсионного фонда:

- бизнес- и технологический процесс, обеспечивающий осуществление специализированным депозитарием контроля за распоряжением имуществом клиентов;
- бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев ценных бумаг (в случае оказания услуг по ведению реестра владельцев инвестиционных паев паевых инвестиционных фондов, ипотечных сертификатов участия).

В.5.9 Осуществление клиринговой деятельности и деятельности центрального контрагента:

- бизнес- и технологический процесс, обеспечивающий определение подлежащих исполнению обязательств;
- бизнес- и технологический процесс, обеспечивающий совершение действий, направленных на исполнение подлежащих исполнению обязательств;
- бизнес- и технологический процесс, обеспечивающий направление поручения на возврат имущества, являющегося клиринговым обеспечением.

В.5.10 Осуществление деятельности организатора торговли:

- бизнес- и технологический процесс, обеспечивающий заключение договора между участниками торгов;
- бизнес- и технологический процесс, обеспечивающий ведение реестров участников торгов и их клиентов, реестра заявок, реестра заключенных на организованных торгах договоров, реестра внебиржевых договоров;
- бизнес- и технологический процесс, обеспечивающий раскрытие и предоставление информации организатора торговли.

В.5.11 Осуществление репозитарной деятельности:

- бизнес- и технологический процесс, обеспечивающий учет заключенных не на организованных торгах договоров РЕПО, договоров, являющихся производными финансовыми инструментами, а также иных договоров;
- бизнес- и технологический процесс, обеспечивающий учет регистратором финансовых транзакций информации о совершении финансовых сделок и об операциях по ним с использованием финансовой платформы;
- бизнес- и технологический процесс, обеспечивающий передачу реестра, ведение которого осуществляет репозитарий, в Банк России или в другой репозитарий.

В.5.12 Осуществление деятельности субъектов страхового дела:

- бизнес- и технологический процесс, обеспечивающий учет страховых случаев;
- бизнес- и технологический процесс, обеспечивающий возврат страховой премии;
- бизнес- и технологический процесс, обеспечивающий работу сайтов в части размещения информации, предусмотренной пунктом 6 статьи 6 Закона Российской Федерации [34].

В.5.13 Осуществление деятельности негосударственных пенсионных фондов:

- бизнес- и технологический процесс, обеспечивающий осуществление выплат вкладчикам, участникам, застрахованным лицам и их правопреемникам негосударственного пенсионного фонда в рамках обязательного пенсионного страхования и негосударственного пенсионного обеспечения;
- бизнес- и технологический процесс, обеспечивающий передачу средств пенсионных резервов и пенсионных накоплений управляющей компании;
- бизнес- и технологический процесс, обеспечивающий перевод выкупных сумм (средств пенсионных накоплений) в иные негосударственные пенсионные фонды и Пенсионный фонд Российской Федерации;
- бизнес- и технологический процесс, обеспечивающий размещение средств пенсионных резервов;
- бизнес- и технологический процесс, обеспечивающий расторжение договора негосударственного пенсионного обеспечения, договора об обязательном пенсионном страховании с негосударственным пенсионным фондом.

В.5.14 Осуществление деятельности операторов инвестиционных платформ:

- бизнес- и технологический процесс, обеспечивающий предоставление доступа к инвестиционной платформе;
- бизнес- и технологический процесс, обеспечивающий размещение инвестиционного предложения;
- бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем предоставления займов;
- бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения эмиссионных ценных бумаг, размещаемых с использованием инвестиционной платформы;
- бизнес- и технологический процесс, обеспечивающий инвестирование с использованием инвестиционной платформы путем приобретения утилитарных цифровых прав;
- бизнес- и технологический процесс, обеспечивающий инвестирование путем приобретения цифровых финансовых активов.

В.5.15 Осуществление деятельности оператора финансовой платформы, включая бизнес- и технологический процесс, обеспечивающий возможность совершения участниками финансовой платформы финансовых сделок с использованием финансовой платформы.

В.5.16 Осуществление деятельности операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов:

- бизнес- и технологический процесс, обеспечивающий доступ к информационной системе, в том числе ведение реестра пользователей информационной системы;
- бизнес- и технологический процесс, обеспечивающий выпуск цифровых финансовых активов в информационной системе;
- бизнес- и технологический процесс, обеспечивающий обращение цифровых финансовых активов в информационной системе, в том числе их погашение записей о цифровых финансовых активах;
- бизнес- и технологический процесс, обеспечивающий внесение записей оператором информационной системы в соответствии с частью 2 статьи 6 Федерального закона [35];
- бизнес- и технологический процесс, обеспечивающий внесение учетных записей в реестр владельцев акций непубличных акционерных обществ, осуществляющих выпуск цифровых финансовых активов, удостоверяющих права участия в капитале указанных непубличных акционерных обществ;
- бизнес- и технологический процесс, обеспечивающий взаимодействие с оператором обмена цифровых финансовых активов;
- бизнес- и технологический процесс, обеспечивающий мониторинг тождественности информации, содержащейся во всех базах данных, составляющих распределенный реестр.

В.5.17 Осуществление деятельности операторов обмена цифровых финансовых активов:

- бизнес- и технологический процесс, обеспечивающий возможность совершения сделок с цифровыми финансовыми активами;
- бизнес- и технологический процесс, обеспечивающий взаимодействие с оператором информационной системы.

В.6 В рамках дополнительной детализации классификации событий риска реализации информационных угроз в разрезе направлений деятельности, в том числе в разрезе составляющих их процессов, финансовая организация классифицирует бизнес- и технологические процессы в разрезе составляющих их технологических участков, определенных в приложении А ГОСТ Р 57580.4—2022.

Приложение Г
(обязательное)

Классификация событий риска реализации информационных угроз в разрезе видов потерь от реализации риска

Г.1 Потери от реализации события риска реализации информационных угроз классифицируются финансовой организацией на прямые и непрямые потери.

Г.2 К прямым потерям финансовой организации относятся потери, отраженные на счетах расходов и убытков в бухгалтерском учете и на приравненных к ним счетах по учету дебиторской задолженности.

Г.3 К непрямым потерям финансовой организации относятся потери, не отраженные в бухгалтерском учете, но косвенно связанные с событиями риска реализации информационных угроз, которые включают:

потери, определяемые расчетным методом в денежном выражении (косвенные потери);

потери, определяемые с использованием экспертного мнения, в случае если потери не выражены в денежном выражении расчетным методом (качественные потери);

потери, не реализовавшиеся в виде прямых и косвенных потерь, которые могли бы возникнуть при реализации не выявленных финансовой организацией источников риска реализации информационных угроз и (или) при неблагоприятном стечении обстоятельств (потенциальные потери).

Г.4 К потенциальным потерям относятся потери (в том числе хищение) средств клиентов, контрагентов, работников и третьих лиц, которые не были компенсированы кредитной организацией, включая потери средств физических лиц, в том числе индивидуальных предпринимателей, юридических лиц, штрафы, наложенные на должностных лиц кредитной организации.

Приложение Д
(обязательное)

Состав КПУР для кредитных организаций

Д.1 Для целей настоящего стандарта состав КПУР для кредитных организаций, определяемый согласно требованиям нормативных актов Банка России [6], распределен по группам, представленным в Д.1.1—Д.1.3.

Д.1.1 Состав группы КПУР, характеризующих уровень совокупных потерь кредитной организации в результате событий риска реализации информационных угроз, приведен в таблице Д.1.

Д.1.2 Состав группы КПУР, характеризующих уровень несанкционированных операций (потерь клиентов) в результате инцидентов, приведен в таблице Д.2.

Д.1.3 Состав группы КПУР, характеризующих уровень зрелости процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, приведен в таблице Д.3.

Д.2 В рамках таблиц Д.1—Д.3 для сигнальных и контрольных значений КПУР, которые кредитная организация определяет самостоятельно, используется обозначение «С» (если иное не установлено нормативными актами Банка России). Для сигнальных и контрольных значений КПУР, которые кредитная организация определяет согласно требованиям нормативных актов Банка России, используется обозначение «ТН».

Таблица Д.1 — Базовый состав группы КПУР, характеризующих уровень совокупных потерь кредитной организации в результате инцидентов

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Общая сумма чистых* прямых потерь от реализации событий риска реализации информационных угроз за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года [6]	С	С
2 Общая сумма валовых** прямых потерь от реализации событий риска реализации информационных угроз, связанных с переводами денежных средств и платежами в платежных системах, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года [6]	С	С
3 Общая сумма валовых прямых и сумм величин косвенных потерь от реализации событий риска реализации информационных угроз 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 риска реализации информационных угроз (в составе операционного риска) на основе статистики базы событий такого риска (с использованием статистики за период не менее пяти лет) с использованием продвинутых подходов [6]	С	С
4 Общая сумма валовых прямых и сумм величин 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) [6]	С	С
5 Общая сумма валовых прямых и сумм величин косвенных потерь кредитной организации в результате переводов и снятия денежных средств, связанных с несанкционированным доступом к объектам информатизации 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) [6]	С	С
6 Отношение общей суммы чистых прямых потерь от реализации событий риска реализации информационных угроз, понесенных кредитной организацией за отчетный период (первый квартал, полугодие, девять месяцев, год), к базовому капиталу кредитной организации на последнюю отчетную дату года [6]	С	С

Окончание таблицы Д.1

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
7 Отношение суммы валовых прямых потерь от реализации событий риска реализации информационных угроз, 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 [6]	ТН	ТН
8 Отношение суммы валовых прямых потерь от реализации событий риска информационной безопасности, связанных с переводами денежных средств и платежами в платежных системах 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 [6]	ТН	ТН
9 Доля реализованных (по количеству), то есть непредотвращенных, событий риска реализации информационных угроз с ненулевой величиной валовых прямых потерь, которые кредитная организация не отразила в базе событий, по отношению ко всем событиям риска реализации информационных угроз, 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*** [6]	С	С
10 Доля выявленных (по количеству) в ходе оценки эффективности функционирования системы управления риском реализации информационных угроз, проведенной уполномоченным подразделением, внешним экспертом или Банком России, событий риска реализации информационных угроз с ненулевой величиной валовых прямых потерь, о которых кредитная организация не сообщила в своих отчетах в Банк России***, к которому относится проверяемый период, по отношению ко всем зарегистрированным событиям риска реализации информационных угроз с ненулевой величиной валовых прямых потерь, о которых кредитная организация сообщила в своих отчетах в Банк России*** [6]	С	С
11 Отношение суммы чистых прямых и сумм величин косвенных потерь от событий риска реализации информационных угроз 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) [6]	С	С
12 Отношение суммы валовых прямых и сумм величин 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) [6]	С	С

* Потери за вычетом суммы возмещения, определяемые с учетом требований нормативных актов Банка России, в частности [6].

** Потери до учета возмещения, определяемые с учетом требований нормативных актов Банка России, в частности [6].

*** Отчеты, направляемые в Банк России в соответствии с пунктом 8 нормативного акта Банка России [8].

Таблица Д.2 — Базовый состав группы КПУР, характеризующих уровень несанкционированных операций в результате инцидентов

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Отношение суммы денежных средств, по которой получены уведомления от клиентов о несанкционированном переводе (списании) денежных средств (в отношении которых получены уведомления от клиентов ОПДС о списании денежных средств с их банковских счетов без их согласия), за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме переводов денежных средств за этот же период [6], [10]	ТН	ТН
2 Отношение суммы денежных средств, возмещенной (возвращенной) клиентам, по которой получены уведомления от клиентов об использовании электронного средства платежа без их согласия в соответствии с частью 11 статьи 9 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств, в отношении которой получены такие уведомления, за этот же период	С	С
3 Отношение количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента — физического лица*, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общему количеству операций по переводу денежных средств за этот же период	С	С
4 Отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к общей сумме денежных средств по операциям по переводу денежных средств за этот же период	С	С
5 Отношение количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены подтверждения клиентов — физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены подтверждения клиентов — физических лиц о возобновлении исполнения распоряжений в соответствии с частью 5.3 статьи 8 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5 статьи 8 Федерального закона [11], за этот же период	С	С

Продолжение таблицы Д.2

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
6 Отношение суммы денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены подтверждения клиентов — физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены подтверждения клиентов — физических лиц о возобновлении исполнения распоряжений в соответствии с частью 5.3 статьи 8 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11], за этот же период	С	С
7 Отношение количества операций по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены уведомления от клиентов — физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к количеству операций по переводу денежных средств без согласия клиента — физического лица** за этот же период	С	С
8 Отношение суммы денежных средств по операциям по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены уведомления от клиентов — физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона [11], за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года к сумме денежных средств по операциям по переводу денежных средств без согласия клиента — физического лица*** за этот же период	С	С

* Операций по переводу денежных средств, соответствующих признакам осуществления перевода денежных средств без согласия клиента — физического лица, размещенным на официальном сайте Банка России в информационно-телекоммуникационной сети Интернет.

** Количество операций по переводу денежных средств без согласия клиента — физического лица должно определяться как сумма количества операций по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены уведомления от клиентов — физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона [11], и количества операций, соответствующих признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11], за исключением случаев, когда получены подтверждения клиентов — физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены подтверждения клиентов — физических лиц о возобновлении исполнения распоряжений в соответствии с частью 5.3 статьи 8 Федерального закона [11].

Окончание таблицы Д.2

*** Сумма денежных средств по операциям по переводу денежных средств без согласия клиента — физического лица должна определяться как сумма денежных средств по операциям по переводу денежных средств, в отношении которых кредитная организация не приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11] и по которым получены уведомления от клиентов — физических лиц об использовании электронного средства платежа без их согласия, в том числе в соответствии с частью 11 статьи 9 Федерального закона [11], и денежных средств по операциям, соответствующим признакам осуществления перевода денежных средств без согласия клиента — физического лица, в отношении которых кредитная организация не приняла к исполнению и (или) приостановила исполнение распоряжений о совершении операций по переводу денежных средств в соответствии с частью 5.1 статьи 8 Федерального закона [11], за исключением случаев, когда получены подтверждения клиентов — физических лиц о направлении распоряжения о совершении операции по переводу денежных средств с их согласия и (или) получены подтверждения клиентов — физических лиц о возобновлении исполнения распоряжений в соответствии с частью 5.3 статьи 8 Федерального закона [11].

Таблица Д.3 — Базовый состав группы КПУР, характеризующих уровень зрелости процессов обеспечения операционной надежности и защиты информации

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Оценка эффективности функционирования системы управления риском реализации информационных угроз, проведенная уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета) кредитной организации [6]	С	С
2 Уровень зрелости процессов применения технологических мер, реализуемых на технологических участках бизнес- и технологических процессов (Оценка выполнения требований нормативных актов Банка России [8], [10], [21] к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации)	С	С
3 Уровень зрелости процессов реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня (Оценка выполнения требований нормативных актов Банка России [8], [10] к обеспечению защиты информации, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений)	С	С
4 Уровень зрелости процессов планирования, реализации, контроля и совершенствования системы защиты информации, определяемой в соответствии с ГОСТ Р 57580.1 (Оценка выполнения требований нормативных актов Банка России [8], [10], [21] к обеспечению защиты информации объектов информатизации согласно методике оценки соответствия, определенной ГОСТ Р 57580.2*) [6]	С	ТН
4.1 Уровень зрелости процесса «Обеспечение защиты информации при управлении доступом», определенного ГОСТ Р 57580.1 (Оценка соответствия уровня защиты информации в отношении указанного процесса согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2)	ТН	ТН
4.2 Уровень зрелости процесса «Предотвращение утечек информации», определенного ГОСТ Р 57580.1 (Оценка соответствия уровня защиты информации в отношении указанного процесса согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2)	ТН	ТН
5 Уровень зрелости процессов планирования, реализации, контроля и совершенствования системы обеспечения операционной надежности финансовой организации, определяемой в соответствии с ГОСТ Р 57580.4 (согласно методике оценки соответствия, определяемой в рамках семейства стандартов ОН)	С	С
* Независимая оценка соответствия уровня защиты информации в отношении объектов информатизации кредитной организации в соответствии с требованиями нормативного акта Банка России [8].		

Приложение Е
(обязательное)

Состав КПУР для некредитных финансовых организаций

Е.1 Для целей настоящего стандарта состав КПУР для некредитных финансовых организаций распределен по группам.

Е.1.1 Состав группы КПУР, характеризующих уровень совокупных потерь некредитной финансовой организации в результате инцидентов, приведен в таблице Е.1.

Е.1.2 Состав группы КПУР, характеризующих уровень несанкционированных операций в результате инцидентов, приведен в таблице Е.2.

Е.1.3 Состав группы КПУР, характеризующих уровень зрелости процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации, приведен в таблице Е.3.

Е.2 В рамках таблиц Е.1—Е.3 для сигнальных и контрольных значений КПУР, которые кредитная организация определяет самостоятельно, используется обозначение «С» (если иное не установлено нормативными актами Банка России). Для сигнальных и контрольных значений КПУР, которые некредитная финансовая организация определяет согласно требованиям нормативных актов Банка России, используется обозначение «ТН».

Таблица Е.1 — Базовый состав группы КПУР, характеризующих уровень совокупных потерь некредитной финансовой организации в результате инцидентов

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Общая сумма валовых прямых потерь от реализации событий риска реализации информационных угроз за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года	С	С
2 Общая сумма валовых прямых и косвенных потерь от реализации событий риска реализации информационных угроз за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года	С	С

Таблица Е.2 — Базовый состав группы КПУР, характеризующих уровень несанкционированных операций в результате инцидентов

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Количество событий реализации информационных угроз, связанных с возникновением финансовых инцидентов, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года	С	С

Таблица Е.3 — Базовый состав группы КПУР, характеризующих уровень зрелости процессов управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Оценка эффективности функционирования системы управления риском реализации информационных угроз, проведенная уполномоченным подразделением и (или) внешним экспертом (специализированной организацией или квалифицированным внешним экспертом) по решению совета директоров (наблюдательного совета), а в случае его отсутствия — исполнительным органом некредитной финансовой организации	С	С
2 Уровень зрелости процессов применения технологических мер, реализуемых на технологических участках бизнес- и технологических процессов (Оценка выполнения требований нормативных актов Банка России [9] к обеспечению защиты информации, применяемых с использованием технологических мер защиты информации)	С	С

Окончание таблицы Е.3

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
3 Уровень зрелости процессов реализации функций безопасности и контроля (наличия) уязвимостей объектов информатизации прикладного уровня (Оценка выполнения требований нормативных актов Банка России [9] к обеспечению защиты информации, применяемых в отношении прикладного программного обеспечения автоматизированных систем и приложений)	С	С
4 Уровень зрелости процессов планирования, реализации, контроля и совершенствования системы защиты информации, определяемой в соответствии с ГОСТ Р 57580.1 (Оценка выполнения требований нормативных актов Банка России [9] к обеспечению защиты информации объектов информатизации согласно методике оценки соответствия, определенной ГОСТ Р 57580.2*)	С	ТН
4.1 Уровень зрелости процесса «Обеспечение защиты информации при управлении доступом», определенного ГОСТ Р 57580.1 (Оценка соответствия уровня защиты информации в отношении указанного процесса согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2)	С	С
4.2 Уровень зрелости процесса «Предотвращение утечек информации», определенного ГОСТ Р 57580.1 (Оценка соответствия уровня защиты информации в отношении указанного процесса согласно методике оценки соответствия защиты информации, определенной ГОСТ Р 57580.2)	С	С
5 Уровень зрелости процессов планирования, реализации, контроля и совершенствования системы обеспечения операционной надежности финансовой организации, определяемой в соответствии с ГОСТ Р 57580.4 (согласно методике оценки соответствия, определяемой в рамках семейства стандартов ОН)	С	ТН
* Независимая оценка соответствия уровня защиты информации в отношении объектов информатизации кредитной организации в соответствии с требованиями нормативного акта Банка России [9].		

Библиография

[1] Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[2] Нормативный акт Банка России, устанавливающий порядок признания Банком России инфраструктурных организаций финансового рынка системно значимыми на основании Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[3] Нормативный акт Банка России, устанавливающий значения критериев для признания платежной системы значимой на основании частей 1 и 2 статьи 22 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[4] Committee on Payments and Market Infrastructures, Board of the International Organization of Securities Commissions. Guidance on cyber resilience for financial market infrastructures. URL: gost.e-ecolog.ru htm (дата обращения: 28.06.2020)

[5] Financial Stability Board. Effective Practices for Cyber Incident Response and Recovery: Consultative document. URL: gost.e-ecolog.ru (дата обращения: 31.03.2021)

[6] Нормативный акт Банка России, устанавливающий требования к системе управления операционным риском в кредитной организации и банковской группе на основании статьи 57.1 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и статьи 11.1-2 Закона Российской Федерации от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»

[7] Федеральный закон от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации»

[8] Нормативный акт Банка России, устанавливающий обязательные для кредитных организаций требования к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента на основании статьи 57.4 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[9] Нормативный акт Банка России, устанавливающий обязательные для некредитных финансовых организаций требования к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций на основании статьи 76.4-1 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[10] Нормативный акт Банка России, устанавливающий требования к обеспечению защиты информации при осуществлении переводов денежных средств и порядок осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств на основании части 3 статьи 27 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[11] Федеральный закон от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[12] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[13] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[14] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[15] Нормативный акт Банка России, устанавливающий требования к системе управления рисками и капиталом кредитной организации и банковской группы на основании Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)» и Закона Российской Федерации от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»

[16] Постановление Правительства Российской Федерации от 3 февраля 2012 г. № 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

[17] ИСО/МЭК 27014:2020 — Информационная безопасность, кибербезопасность и защита конфиденциальности. Управление информационной безопасностью (Information security, cybersecurity and privacy protection — Governance of information security)

[18] Закон Российской Федерации от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»

[19] Федеральный закон от 26 декабря 1995 г. № 208-ФЗ «Об акционерных обществах»

[20] Рекомендации в области стандартизации Банка России РС БР ИББС-2.2-2009 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности

[21] Нормативный акт Банка России, устанавливающий требования к защите информации в платежной системе Банка России на основании пункта 19 части 1 и части 9 статьи 20 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[22] Рекомендации в области стандартизации Банка России РС БР ИББС-2.7-2015 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Ресурсное обеспечение информационной безопасности

[23] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, разработанный в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[24] Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, разработанных в соответствии с частью 4 статьи 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[25] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, разработанные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[26] Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, разработанные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[27] Стандарт Банка России СТО БР ИББС-1.4-2018 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Управление риском нарушения информационной безопасности при аутсорсинге

[28] Стандарт Банка России СТО БР ФАПИ.СЕК-1.6-2020 — Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы обеспечения безопасности финансовых сервисов на основе протокола OpenID. Требования

[29] Стандарт Банка России СТО БР ФАПИ.ПАОК-1.0-2021 — Безопасность финансовых (банковских) операций. Прикладные программные интерфейсы. Обеспечение безопасности финансовых сервисов при инициации OpenID Connect клиентом потока аутентификации по отдельному каналу. Требования

[30] Рекомендации в области стандартизации Банка России РС БР ИББС-2.5-2014 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности

[31] Стандарт Банка России СТО БР ИББС-1.3-2016 — Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Сбор и анализ технических данных при реагировании на инциденты информационной безопасности при осуществлении переводов денежных средств

[32] Стандарт Банка России СТО БР БФБО-1.5-2018 — Безопасность финансовых (банковских) операций. Управление инцидентами информационной безопасности. О формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации

[33] Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»

[34] Закон Российской Федерации от 27 ноября 1992 г. № 4015-1 «Об организации страхового дела в Российской Федерации»

[35] Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации»

[36] Нормативный акт Банка России о требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков на основании пунктов 4—6 части 3 статьи 28 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

УДК 004.056.5:006.354

ОКС 03.060
35.030

Ключевые слова: управление риском реализации информационных угроз и обеспечение операционной надежности, система управления риском реализации информационных угроз, уровень защиты, требования к системе управления риском реализации информационных угроз

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 23.12.2022. Подписано в печать 09.01.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 12,56. Уч.-изд. л. 11,30.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru