ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57580.4— 2022

Безопасность финансовых (банковских) операций

ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Базовый состав организационных и технических мер

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. № 1549-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 1
3 Термины и определения 2
4 Сокращения 3
5 Структура стандарта 4
6 Общие положения 4
7 Требования к системе обеспечения операционной надежности финансовой организации 7
7.1 Общие положения 7
7.2 Процесс 1 «Идентификация критичной архитектуры» 8
7.3 Процесс 2 «Управление изменениями» 10
7.4 Процесс 3 «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации» 17
7.5 Процесс 4 «Взаимодействие с поставщиками услуг» 29
7.6 Процесс 5 «Тестирование операционной надежности бизнес- и технологических процессов» 33
7.7 Процесс 6 «Защита критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы» 36
7.8 Процесс 7 «Управление риском внутреннего нарушителя» 37
7.9 Процесс 8 «Обеспечение осведомленности об актуальных информационных угрозах» 39
8 Требования к системе организации и управления операционной надежностью финансовой организации 42
8.1 Общие положения 42
8.2 Направление 1 «Планирование процесса системы обеспечения операционной надежности» 42
8.3 Направление 2 «Реализация процесса системы обеспечения операционной надежности» 43
8.4 Направление 3 «Контроль процесса системы обеспечения операционной надежности» . . . 44
8.5 Направление 4 «Совершенствование процесса системы обеспечения операционной надежности» 45
Приложение А (справочное) Перечень технологических мер защиты информации 47
Приложение Б (обязательное) Целевые показатели операционной надежности 48
Библиография 49

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]. Одно из условий достижения этих целей — должная реализация в кредитных организациях, некредитных финансовых организациях Российской Федерации, а также в субъектах национальной платежной системы (далее — финансовые организации) процессов обеспечения операционной надежности в условиях возможной реализации информационных угроз (далее — операционная надежность) при осуществлении видов деятельности, связанных с предоставлением финансовых, банковских услуг, в том числе услуг по осуществлению переводов денежных средств (далее — финансовые услуги), и (или) информационных услуг.

Применение информационных технологий для финансовых организаций стало основополагающей и неотъемлемой составляющей предоставления финансовых и (или) информационных услуг. Возникла зависимость устойчивого функционирования и развития финансовых организаций от надлежащего использования информационных технологий. В то же время деятельность финансовых организаций подвержена множеству разнообразных информационных угроз, реализация которых, как правило, приводит к финансовым (банковским) операциям, в том числе к переводам денежных средств, без согласия клиента, а также к нарушению надлежащего предоставления финансовых и (или) информационных услуг. В свою очередь, это оказывает влияние на операционную надежность финансовой организации и может приводить к следующим негативным последствиям:

- к возникновению потерь финансовой организации, причастных сторон, в том числе клиентов финансовой организации, в результате инцидентов, связанных с реализацией информационных угроз (далее — инциденты);
- нарушению непрерывного предоставления финансовой организацией финансовых и (или) информационных услуг;
- невыполнению обязательств по обеспечению защиты интересов клиентов финансовой организации;
- несоблюдению 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 [2], а также устанавливаемых статьей 19 Федерального закона [3], статьей 16 Федерального закона [4] и Федеральным законом [5].

Реализация информационных угроз может также приводить к крупномасштабным инцидентам в пределах финансовой экосистемы, банковской системы, финансового рынка Российской Федерации и (или) национальной платежной системы. Если инцидент, обладающий потенциалом крупномасштабного, не локализован, его реализация может охватить различные финансовые организации, финансовые объединения и финансовые экосистемы, а также используемые ими объекты информатизации, в том числе входящие в критичную архитектуру. В свою очередь, это может привести к негативным последствиям, указанным выше, в рамках функционирования финансовой системы в целом, причиняя при этом значительный ущерб репутации ряда финансовых организаций.

Операционная надежность финансовой организации определяется также наличием взаимосвязей и (или) взаимозависимостей бизнес- и технологических процессов финансовой организации и причастных сторон, что в случае возникновения нарушений может приводить к потере доверия к финансовой организации или к возникновению дополнительной нагрузки на капитал финансовой организации вследствие возникновения существенных потерь в результате инцидентов.

Эффективное и результативное выявление, реагирование на инциденты и восстановление функционирования бизнес- и технологических процессов и объектов информатизации после произошедших инцидентов имеют важное значение для минимизации негативного влияния риска реализации информационных угроз и обеспечения операционной надежности финансовой организации.

Надежность, доступность и способность восстановления в кратчайшие сроки функционирования бизнес- и технологических процессов, включая восстановление задействованных при их выполнении объектов информатизации, являются ключевыми факторами повышения доверия причастных сторон, в том числе клиентов финансовой организации, к операционным возможностям финансовой организации.

Одними из источников риска реализации информационных угроз являются уязвимости задействованных при выполнении бизнес- и технологических процессов объектов информатизации. При этом

из-за возможного наличия уязвимостей нулевого дня[1)] потенциально уязвимым может оказаться любой объект информатизации. Уменьшению негативного влияния риска реализации информационных угроз в таком случае способствуют меры, направленные на реализацию следующих процессов:

- выявление, регистрация, реагирование на инциденты и восстановление после их реализации;
- тестирование операционной надежности бизнес- и технологических процессов, включающее сценарный анализ и тестирование готовности финансовой организации противостоять реализации информационных угроз.

При этом обеспечение устойчивого выполнения бизнес- и технологических процессов, а также устойчивого функционирования задействованных при их выполнении объектов информатизации в условиях возможной реализации информационных угроз в настоящее время является одним из основных факторов сохранения конкурентоспособности в условиях цифровизации экономики.

Основными целями настоящего стандарта являются:

- определение перечня процессов и соответствующих требований к составу и содержанию мер, направленных на обеспечение операционной надежности финансовыми организациями;
- достижение адекватности состава и содержания мер, направленных на обеспечение операционной надежности финансовыми организациями актуальным информационным угрозам и допустимому уровню риска реализации информационных угроз, принятому финансовой организацией;
- содействие эффективному и стандартизованному контролю мероприятий по обеспечению операционной надежности.

[1)] Термин применен в значении, установленном 3.8 ГОСТ Р 56545—2015.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Безопасность финансовых (банковских) операций

ОБЕСПЕЧЕНИЕ ОПЕРАЦИОННОЙ НАДЕЖНОСТИ

Базовый состав организационных и технических мер

Security of financial (banking) operations.
Ensuring operational resilience.
Basic set of organizational and technical measures

Дата введения — 2023—02—01

1 Область применения

Настоящий стандарт устанавливает требования к составу и содержанию мер обеспечения операционной надежности для тех уровней защиты, которые применяют финансовые организации при определении базового состава таких мер.

Настоящий стандарт служит для целей содействия соблюдения требований и рассматривается в качестве дополнения к нормативным актам Банка России, устанавливающих требования к системе управления операционным риском [6], а также требования к операционной надежности [7], [8].

Положения настоящего стандарта предназначены для использования кредитными организациями, некредитными финансовыми организациями, указанными в части первой 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 негативных последствий для бесперебойности функционирования платежной системы, а также надлежащего оказания услуг банкам и их клиентам рекомендуется применять меры обеспечения операционной надежности, определяемые настоящим стандартом.

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 и (или) информационных услуг.

Состав мер обеспечения операционной надежности, определяемый настоящим стандартом, применим к совокупности критичных активов, идентифицируемых в рамках процесса «Идентификация критичной архитектуры».

Область применения настоящего стандарта, определяющая обязанность финансовых организаций внедрять меры обеспечения операционной надежности, реализующие один из уровней защиты для совокупности критичных активов финансовой организации, устанавливается в нормативных актах Банка России путем включения нормативной ссылки на настоящий стандарт, приводимой на основании статьи 27 Федерального закона [9].

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 договорах.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

Издание официальное

ГОСТ Р 53647.1—2009 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство

ГОСТ Р 53647.2—2009 Менеджмент непрерывности бизнеса. Часть 2. Требования

ГОСТ Р 53647.3—2015 Менеджмент непрерывности бизнеса. Часть 3. Руководство по обеспечению соответствия требованиям ГОСТ Р ИСО 22301

ГОСТ Р 53647.4—2011/ISO/PAS 22399:2007 Менеджмент непрерывности бизнеса. Руководящие указания по обеспечению готовности к инцидентам и непрерывности деятельности

ГОСТ Р 55235.3—2012 Практические аспекты менеджмента непрерывности бизнеса. Применение к информационным и коммуникационным технологиям

ГОСТ Р 56545—2015 Защита информации. Уязвимости информационных систем. Правила описания уязвимостей

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

ГОСТ Р 57580.3—2022 Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения

ГОСТ Р 58256—2018 Защита информации. Управление потоками информации в информационной системе. Формат классификационных меток

ГОСТ Р ИСО 22301—2014 Надежность в технике. Системы менеджмента непрерывности бизнеса. Общие требования

ГОСТ Р ИСО 22313—2015 Менеджмент непрерывности бизнеса. Руководство по внедрению

ГОСТ Р ИСО 28000—2019 Технические условия для систем менеджмента безопасности цепи поставок

ГОСТ Р ИСО/МЭК 27036-2—2020 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования

ГОСТ Р ИСО/МЭК 27036-4—2020 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, 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 термины по ГОСТ Р 57580.1 и ГОСТ Р 57580.3, а также следующие термины с соответствующими определениями:

3.1 **целевая точка восстановления данных;** ЦТВД: Состояние (объем), до которого необходимо восстановить данные, используемые в рамках выполнения бизнес- и технологических процессов, связанных с предоставлением финансовых и (или) информационных услуг, для обеспечения возобновления их выполнения.

Примечание — Адаптировано из ГОСТ Р ИСО 22301—2014.

3.2 **целевое время восстановления;** ЦВВ: Период времени, установленный финансовой организацией для возобновления предоставления финансовых и (или) информационных услуг, выполняемых при этом бизнес- и технологических процессов или восполнения ресурсов после инцидента, связанного с реализацией информационных угроз.

Примечания

1 Адаптировано из ГОСТ Р ИСО 22301—2014.

2 Для бизнес- и технологических процессов целевое время восстановления не должно превышать допустимого времени простоя и (или) деградации бизнес- и технологических процессов.

3 Операторам услуг платежной инфраструктуры при установлении целевого времени восстановления следует учитывать требования к определению показателя продолжительности восстановления оказания услуг платежной инфраструктуры согласно нормативному акту Банка России [10].

3.3 **техническая мера обеспечения операционной надежности:** Мера, реализуемая с помощью применения аппаратных, программных, аппаратно-программных средств и (или) систем.

3.4 **организационная мера обеспечения операционной надежности:** Мера, не являющаяся технической мерой обеспечения операционной надежности, предусматривающая установление регламента работы с элементами критичной архитектуры и порядка фиксации результатов выполненной работы, в том числе установление в отдельных случаях временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования, и режимы работы объекта информатизации и (или) иных связанных с ним объектов.

3.5 **конфигурация объекта информатизации:** Совокупность параметров, определяющих структуру (совокупность функциональных частей и их взаимосвязь) и условия функционирования объекта информатизации.

3.6 **система обеспечения операционной надежности:** Совокупность организационных и технических мер, применение которых направлено на непосредственное обеспечение операционной надежности, процессов применения указанных мер, ресурсного и организационного обеспечения, необходимого для их применения.

3.7 **система организации и управления операционной надежностью:** Совокупность мер, применением которых достигается полнота и качество обеспечения операционной надежности, предназначенных для планирования, реализации, контроля и совершенствования процессов системы обеспечения операционной надежности.

3.8 **допустимое время простоя и (или) деградации бизнес- и технологических процессов:** Допустимый для финансовой организации временной период, в течение которого происходит простой и (или) деградация бизнес- и технологических процессов.

3.9 **допустимая доля деградации бизнес- и технологического процесса:** Допустимое отношение общего количества финансовых (банковских) операций, в том числе операций по переводу денежных средств и (или) иных операций в рамках технологических операций (участков) бизнес- и технологических процессов, совершенных во время деградации бизнес- и технологического процесса в рамках инцидента к ожидаемому количеству операций за тот же период в случае непрерывного оказания услуг, установленного финансовой организацией.

Примечания

1 Под деградацией бизнес- и технологических процессов следует понимать нарушение технологических процессов, приводящих к неоказанию и (или) ненадлежащему оказанию финансовых и (или) информационных услуг.

2 Финансовая организация рассчитывает значение допустимой доли деградации на основании статистических данных за период не менее 12 календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности и (или) иных данных, обосновывающих их определение (по выбору финансовой организации).

Если технологический процесс функционирует менее 12 календарных месяцев, финансовые организации определяют значение допустимой доли деградации технологических процессов на основании статистических данных за период с даты начала его функционирования и (или) иных данных, обосновывающих их определение (по выбору финансовой организации).

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ИБ — информационная безопасность;

КПУР — контрольный показатель уровня риска реализации информационных угроз;

ПО — программное обеспечение;

СВР — степень возможности реализации;

СТП — степень тяжести последствий;

BIA — анализ воздействия на деятельность (business impact analysis);
SLA — соглашение об уровне обслуживания (service level agreement);
NDA — соглашение о неразглашении информации (non-disclosure agreement).

5 Структура стандарта

Настоящий стандарт входит в состав комплекса национальных стандартов «Безопасность финансовых (банковских) операций»[1)] (далее — комплекс стандартов) и содержит описание систем:

- обеспечения операционной надежности;
- организации и управления обеспечения операционной надежности.

Настоящий стандарт раскрывает отдельные разделы базового в рамках комплекса стандартов ГОСТ Р 57580.3, содержащего соответствующие ссылки на нижеприведенные разделы настоящего стандарта.

Раздел 6 «Общие положения» содержит общие положения и рекомендации по реализации финансовой организацией процессов системы обеспечения операционной надежности.

Раздел 7 «Требования к системе обеспечения операционной надежности финансовой организации» содержит требования к содержанию базового состава мер обеспечения операционной надежности, применение которых направлено на непосредственное обеспечение операционной надежности для каждого из уровней защиты.

Раздел 8 «Требования к системе организации и управлению операционной надежностью финансовой организации» содержит для каждого из уровней защиты требования к содержанию базового состава мер обеспечения операционной надежности, направленных на обеспечение должной зрелости (полноты и качества) реализации системы обеспечения операционной надежности.

Приложение А «Перечень технологических мер защиты информации» содержит перечень технологических мер защиты информации, обрабатываемой в рамках технологических операций (участков) при выполнении бизнес- и технологических процессов финансовой организации.

Приложение Б «Целевые показатели операционной надежности» содержит базовый состав целевых показателей операционной надежности и информацию по установлению их сигнальных и контрольных значений.

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 снижения риска и противодействия реализации информационных угроз, а также их влиянию на операционную надежность финансовой организации следует, среди прочего, обеспечить должное планирование, реализацию, контроль и совершенствование процессов системы обеспечения операционной надежности.

6.2 Планирование и реализация процессов обеспечения операционной надежности должны быть осуществлены финансовой организацией на всех этапах жизненного цикла элементов критичной архитектуры, начиная с этапа разработки и планирования внедрения бизнес- и технологических процессов, реализующих виды деятельности финансовой организации, связанные с предоставлением финансовых и (или) информационных услуг.

Указанный подход позволяет удостовериться в эффективности, защищенности и устойчивости реализуемых бизнес- и технологических процессов.

6.3 Организационная структура управления процессами обеспечения операционной надежности реализуется в соответствии с требованиями нормативных актов Банка России, в частности [6], и положениями ГОСТ Р 57580.3 и является составляющей частью более широкой организационной структуры управления финансовой организации. Цели и приоритеты обеспечения операционной надежности должны соответствовать целям и приоритетам управления рисками (операционным риском), в том числе риском реализации информационных угроз, установленным в финансовой организации, и должны

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

быть доведены до сведения всех вовлеченных подразделений и должностных лиц финансовой организации.

Принимаемые исполнительным органом решения, связанные с обеспечением достижения целей и приоритетов операционной надежности финансовой организации, должны соответствовать общим бизнес-целям финансовой организации.

6.4 Процессы обеспечения операционной надежности существенным образом связаны с поддержанием непрерывности деятельности и ее восстановлением после возможных прерываний. При этом на обеспечение операционной надежности значительное влияние оказывают проектирование, реализация и управление критичными активами в соответствии с установленными показателями операционной надежности, в том числе разработка и (или) применение технических решений, функциональные возможности и характеристики которых соответствуют потребностям финансовой организации по обеспечению непрерывности и качества функционирования объектов информатизации, входящих в критичную архитектуру.

Наряду с мерами обеспечения операционной надежности, приведенными в разделе 7, финансовым организациям следует рассматривать следующие вопросы:

а) проведение сценарного анализа (в части возможного прерывания деятельности финансовой организации в результате реализации инцидентов в отношении критичных активов), проведение анализа влияния на бизнес (BIA) с учетом результатов сценарного анализа, а также установление ЦВВ и ЦТВД в отношении критичных активов;

б) проектирование и реализацию критичных активов в исполнении, позволяющем ограничить негативное воздействие в результате инцидентов и восстановить предоставление финансовых и (или) информационных услуг в течение заданного временного периода (ЦВВ), в том числе завершить расчеты к концу операционного дня, а также обеспечить целостность защищаемой информации[1)], связанной с осуществлением финансовых (банковских) операций, в том числе переводов денежных средств;

в) обеспечение необходимой и достаточной производительности объектов информатизации финансовой организации, их надежной работы (отказоустойчивости), возможности их планового масштабирования, а также оперативного восстановления работоспособности;

г) применение отказоустойчивых решений, разделение основных и резервных критичных активов (в том числе в части их резервирования[2)]), используемых в рамках обработки и хранения данных, достигаемое в том числе:

1) созданием резервных центров обработки и хранения данных, обеспечением защиты информации резервных центров обработки и хранения данных на уровне, эквивалентном основным центрам,

2) раздельным размещением основного и резервного центров обработки и хранения данных для снижения подверженности однотипным угрозам,

3) подготовкой и тестированием готовности резервных центров обработки и хранения данных к выполнению определенных финансовой организацией бизнес- и технологических процессов,

4) определением резервных каналов связи и электроснабжения в основных и резервных центрах обработки и хранения данных с обеспечением их максимального разделения для снижения вероятности их выхода из строя,

5) привлечением поставщиков услуг (в том числе поставщиков облачных услуг), имеющих более одного центра обработки данных.

Примечания

1 Инфраструктурным организациям финансового рынка[3)] следует обеспечивать возможность восстановления выполнения бизнес- и технологических процессов на резервных площадках, которые обеспечены необходимыми ресурсами для восстановления бизнес- и технологических процессов на заранее заданном уровне.

В зависимости от важности и уровня взаимосвязанности инфраструктурным организациям финансового рынка рекомендуется предусматривать как минимум двукратное резервирование для таких площадок на случай реализации сценариев, при которых основная и резервная площадки могут оказаться недоступными [15]. Одно-

---

1) К защищаемой информации относится информация, перечень которой определен в [11]—[13].

2) Включая системы резервного хранения, электро- и холодоснабжения/теплоотвода, каналы связи.

3) В рамках настоящего стандарта под инфраструктурными организациями финансового рынка понимаются организации, определенные в рамках нормативных актов Банка России [14] (финансовые организации, осуществляющие деятельность центрального контрагента, центрального депозитария, расчетного депозитария, репозитария).

временно с этим при организации резервных площадок рекомендуется учитывать географическое расположение филиалов и региональных офисов.

2 В качестве дополнительных мер, направленных на поддержание эквивалентного уровня вычислительных мощностей при использовании резервных центров обработки и хранения данных, рекомендуется предусмотреть возможность распределения нагрузки на вычислительные мощности между такими резервными объектами и основными центрами обработки и хранения данных, не подвергшимися влиянию информационных угроз (при их наличии), или двукратное резервирование за счет «законсервированных» объектов, которые обеспечены необходимыми ресурсами для восстановления бизнес- и технологических процессов на заранее заданном уровне.

3 В случае привлечения поставщиков услуг (в том числе поставщиков облачных услуг) в целях резервирования объектов информатизации инфраструктурного уровня рекомендуется предусмотреть резервирование всех компонентов таких объектов информатизации с учетом возможностей и специфики поставщика услуг;

д) обеспечение целостности и доступности данных, необходимых для реализации бизнес- и технологических процессов, достигаемое в том числе:

1) установлением во внутренних документах и применением соответствующих политик (режимов) резервного копирования и восстановления данных, определяющих, как минимум, частоту и объем резервного копирования [в том числе с учетом значимости и частоты обновления (ввода новых) данных],

2) разработкой политик (режимом) резервного копирования и восстановления данных, обеспечивающих быстрое восстановление и минимальный уровень простоя и (или) деградации бизнес- и технологических процессов,

3) резервированием на регулярной основе всех данных, необходимых для восстановления (воспроизведения) данных об осуществленных финансовых (банковских) операциях, в том числе операциях по переводу денежных средств,

4) реализацией процедур восстановления (воспроизведения) данных об осуществленных финансовых (банковских) операциях, в том числе операциях по переводу денежных средств, которые могут включать возвращение к исходным данным о таких операциях («откат») и ведение журнала совершаемых операций;

е) разработка и тестирование плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности финансовой организации в случае возникновения прерываний (План ОНиВД).

Указанные вопросы в значительной степени влияют на обеспечение операционной надежности. Установление состава организационных и технических мер в отношении процессов (действий), указанных в перечислениях данного пункта, не является предметом настоящего стандарта. Для организации таких процессов (действий) следует руководствоваться требованиями нормативных актов Банка России (в частности, [6]), а также рекомендуется руководствоваться положениями ГОСТ Р ИСО 22301, ГОСТ Р ИСО 22313, ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р 53647.1, ГОСТ Р 53647.2, ГОСТ Р 53647.3, ГОСТ Р 53647.4, ГОСТ Р 55235.3, а также [16], [17]. При этом при реализации положений настоящего стандарта в финансовой организации целесообразно применять подход, предполагающий интеграцию процессов обеспечения операционной надежности и процессов обеспечения непрерывности и (или) восстановления деятельности в случае возникновения прерываний.

6.5 Выбор и применение финансовой организацией мер обеспечения операционной надежности включает:

- выбор мер обеспечения операционной надежности, требования к составу и содержанию которых установлены в разделе 7;

- адаптацию (уточнение), при необходимости, выбранного состава и содержания мер обеспечения операционной надежности с учетом модели угроз и нарушителей безопасности информации финансовой организации и структурно-функциональных характеристик объектов информатизации, включаемых в область применения настоящего стандарта;

- исключение из выбранного состава мер, не связанных с используемыми информационными технологиями;

- дополнение, при необходимости, адаптированного (уточненного) состава и содержания мер обеспечения операционной надежности мерами, которые необходимы для обработки актуальных информационных угроз, закрепленных в модели угроз безопасности информации финансовой организации, в том числе обеспечения выполнения требований, установленных нормативными правовыми актами [18]—[20];

- применение для конкретной области адаптированного (уточненного) и дополненного состава мер обеспечения операционной надежности в соответствии с положениями раздела 8.

6.6 При невозможности технической реализации отдельных выбранных мер обеспечения операционной надежности, а также с учетом экономической целесообразности на этапах адаптации (уточнения) состава мер могут быть разработаны иные (компенсирующие) меры, направленные на нейтрализацию информационных угроз, определенных в модели информационных угроз, и действий нарушителей безопасности информации финансовой организации.

В этом случае финансовой организацией должно быть приведено обоснование применения компенсирующих мер обеспечения операционной надежности.

Применение компенсирующих мер обеспечения операционной надежности должно быть направлено на обработку риска, связанного с реализацией тех же информационных угроз, на нейтрализацию которых направлены меры из исходного состава мер обеспечения операционной надежности настоящего стандарта, не применяемые финансовой организацией в связи с невозможностью технической реализации и (или) экономической целесообразностью.

6.7 Снижение риска реализации информационных угроз в целях обеспечения операционной надежности финансовой организации обеспечивается путем надлежащего выбора, повышения полноты и качества применения соответствующих мер обеспечения операционной надежности. Полнота и качество применения мер обеспечения операционной надежности достигаются планированием, реализацией, контролем и совершенствованием системы обеспечения операционной надежности, осуществляемыми в рамках системы организации и управления операционной надежностью.

6.8 Настоящий стандарт определяет три уровня защиты:

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

Уровень защиты для финансовой организации применяется согласно критериям, устанавливаемым нормативными актами Банка России с учетом:

- вида деятельности финансовой организации, состава предоставляемых финансовой организацией финансовых и (или) информационных услуг, реализуемых бизнес- и технологических процессов;
- объема финансовых (банковских) операций, в том числе операций по переводу денежных средств;
- размера организации, например 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.

6.9 Финансовой организации следует применить риск-ориентированный подход и определить приоритеты по реализации мер обеспечения операционной надежности таким образом, чтобы данные меры отвечали принятому финансовой организацией допустимому уровню риска реализации информационных угроз (риск-аппетиту), а также были адекватны информационным угрозам и оптимальны с точки зрения рисков и ресурсов для реализации.

7 Требования к системе обеспечения операционной надежности финансовой организации

7.1 Общие положения

7.1.1 Настоящий раздел устанавливает требования к мерам по обеспечению операционной надежности финансовой организации для следующих процессов обеспечения операционной надежности:

а) процесс 1 «Идентификация критичной архитектуры»;

б) процесс 2 «Управление изменениями»;

в) процесс 3 «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации»;

г) процесс 4 «Взаимодействие с поставщиками услуг»;

д) процесс 5 «Тестирование операционной надежности бизнес- и технологических процессов»;

е) процесс 6 «Защита критичной архитектуры от возможной реализации информационных угроз при организации удаленной работы»;

ж) процесс 7 «Управление риском внутреннего нарушителя»;

и) процесс 8 «Обеспечение осведомленности об актуальных информационных угрозах».

7.1.2 Способы реализации мер по обеспечению операционной надежности, установленные в таблицах 1—17, обозначены следующим образом:

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

7.2 Процесс 1 «Идентификация критичной архитектуры»

7.2.1 Применяемые финансовой организацией меры по идентификации критичной архитектуры должны обеспечивать организацию учета и контроля состава элементов критичной архитектуры.

7.2.2 Состав мер по организации учета и контроля состава элементов критичной архитектуры применительно к уровням защиты приведен в таблице 1.

Таблица 1

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ИКА.1	Организация* и выполнение деятельности по учету элементов критичной архитектуры:			
ИКА.1.1	- бизнес- и технологических процессов**, реализуемых непосредственно финансовой организацией	О	О	Т
ИКА.1.2	- бизнес- и технологических процессов, технологических операций (участков), реализуемых поставщиками услуг [переданных на аутсорсинг и (или) выполняемых с применением сторонних информационных сервисов, предоставляемых поставщиками услуг]	О	О	Т
ИКА.1.3	- подразделений финансовой организации, ответственных за разработку бизнес- и технологических процессов, поддержание их реализации бизнес- и технологических процессов	О	О	Т
ИКА.1.4	- технологических операций (участков) в рамках каждого из бизнес- и технологического процессов	Н	О	Т
ИКА.1.5	- объектов информатизации (прикладного и инфраструктурного уровней) финансовой организации, задействованных при выполнении каждого из бизнес- и технологического процессов, в том числе их конфигураций	О	Т	Т
ИКА.1.6	- субъектов доступа, задействованных при выполнении каждого из бизнес- и технологического процессов	О	Т	Т
ИКА.1.7	- взаимосвязей и взаимозависимостей между финансовой организацией и причастными сторонами (за исключением клиентов финансовой организации) в рамках выполнения бизнес- и технологических процессов	Н	О	Т
ИКА.1.8	- каналов передачи (информационных потоков) защищаемой информации***, обрабатываемой и передаваемой в рамках бизнес- и технологических процессов	Н	О	Т
ИКА.2	Организация и выполнение деятельности по классификации технологических операций (участков) бизнес- и технологического процессов, значимых в контексте необходимости применения технологических мер защиты информации в соответствии с приложением А	Н	О	Т
ИКА.3	Организация и выполнение деятельности по классификации объектов информатизации инфраструктурного уровня, как минимум, по следующим системным уровням:	О	О	Т

[1)] По решению финансовой организации способ «О» может быть реализован путем применения технической меры обеспечения операционной надежности в дополнение или взамен применения организационной меры обеспечения операционной надежности.

Продолжение таблицы 1

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ИКА.3	- уровень аппаратного обеспечения; - уровень сетевого оборудования; - уровень сетевых приложений и сервисов; - уровень серверных компонентов виртуализации, программных инфраструктурных сервисов; - уровень операционных систем, систем управления базами данных, серверов приложений	О	О	Т
ИКА.4	Организация и выполнение деятельности по классификации объектов информатизации прикладного уровня (прикладного ПО автоматизированных систем и приложений), значимых в контексте отсутствия уязвимостей, как минимум по следующим типам: - прикладное ПО автоматизированных систем и приложения финансовой организации, отвечающие критериям доступности из сети Интернет; - прикладное ПО автоматизированных систем и приложения, передаваемые клиентам финансовой организации для установки на их технические средства	О	О	Т
ИКА.5	Организация и выполнение деятельности по классификации субъектов доступа по принадлежности работников к группе повышенного риска, обладающих привилегированным доступом к объектам информатизации, задействованным при выполнении бизнес- и технологических процессов	О	О	Т
ИКА.6	Организация и выполнение деятельности по учету и классификации сервисов поставщика облачных услуг и применяемых мер защиты информации в зависимости от модели предоставления сервиса: - SaaS (Software as a service) — ПО как услуга; - PaaS (Platform as a service) — платформа как услуга; - IaaS (Infrastructure as a service) — инфраструктура как услуга	Н	О	Т
ИКА.7	Организация и выполнение деятельности по классификации защищаемой информации (определению критериев отнесения информации к защищаемой и перечня ее типов), обрабатываемой, передаваемой и (или) хранимой финансовой организацией в рамках выполнения бизнес- и технологических процессов в соответствии с требованиями законодательства Российской Федерации, в том числе нормативных актов Банка России [11]—[13]	О	О	Т
ИКА.8	Организация и выполнение деятельности по классификации в зависимости от класса обрабатываемой, передаваемой и (или) хранимой защищаемой информации задействованных при этом:			
ИКА.8.1	- объектов информатизации	О	О	Т
ИКА.8.2	- субъектов доступа	О	О	Т
ИКА.8.3	- каналов передачи (информационных потоков) защищаемой информации как внутри финансовой организации, так при взаимодействии с причастными сторонами	Н	О	Т
ИКА.9	Организация и выполнение деятельности по фиксации результатов учета и классификации, предусмотренных мерами ИКА.1 — ИКА.8, с использованием стандартизованных нотаций описания (например, BPMN [21], TOGAF [22])	Н	Н	Т
ИКА.10	Организация и выполнение деятельности по единому централизованному учету результатов идентификации и классификации, предусмотренных мерами ИКА.1 — ИКА.8	Н	Н	Т

Окончание таблицы 1

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ИКА.11	Установление во внутренних документах финансовой организации для каждого из бизнес- и технологического процессов, входящих в критичную архитектуру, целевых показателей операционной надежности согласно приложению Б	О	О	О
ИКА.12	Контроль состава [обеспечение актуальности данных (инвентарных)] критичных активов (элементов критичной архитектуры)*4:			
ИКА.12.1	- контроль состава критичных активов (элементов критичной архитектуры), учет которых предусмотрен мерами ИКА.1.1—ИКА.1.3	О	О	О
ИКА.12.2	- контроль состава критичных активов (элементов критичной архитектуры), учет которых предусмотрен мерами ИКА.1.4 и ИКА.1.7	Н	О	О
ИКА.12.3	- контроль состава критичных активов (элементов критичной архитектуры), учет которых предусмотрен мерами ИКА.1.5 и ИКА.1.6	О	Т	Т
ИКА.12.4	- контроль состава критичных активов (элементов критичной архитектуры), учет которых предусмотрен мерой ИКА.1.8	Н	О	Т
ИКА.13	Организация и выполнение деятельности по описанию актуальной топологии вычислительных сетей финансовой организации*5	Н	О	Т

* Организация деятельности должна включать отражение во внутренних документах финансовой организации регламента осуществления соответствующей деятельности и распределения ролей по ее выполнению.

** Перечень бизнес- и технологических процессов, обязательных для включения в критичную архитектуру, устанавливается нормативными актами Банка России [7], [8].

*** Рекомендуется использовать ГОСТ Р 58256.

*4 В целях обеспечения актуальности данных (инвентарных) о критичных активах (элементах критичной архитектуры) процесс идентификации критичной архитектуры должен быть интегрирован с процессом управления изменениями, а также реализован на этапах жизненного цикла объектов информатизации.

*5 Описание топологии вычислительных сетей финансовой организации должно, как минимум, содержать информацию о сетевом расположении (как минимум, ip-адресах):

- сетевых роутеров;
- средств защиты информации;
- серверных устройств, задействованных в выполнении бизнес- и технологических процессов;
- иных объектов информатизации, задействованных в реализации бизнес- и технологических процессов и (или) непосредственно взаимодействующих с сетью Интернет.

В случае привлечения поставщика облачных услуг описание топологии должно содержать информацию только о сетевом расположении устройств, находящихся под управлением финансовой организации.

7.3 Процесс 2 «Управление изменениями»

7.3.1 Применяемые финансовой организацией меры по управлению изменениями должны обеспечивать:

а) организацию и выполнение процедур управления изменениями в критичной архитектуре, направленных:

1) на управление уязвимостями в критичной архитектуре, с использованием которых могут быть реализованы информационные угрозы и которые могут повлечь превышение значений целевых показателей операционной надежности,

2) планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение недопустимости неоказания или ненадлежащего оказания финансовых (банковских) услуг;

б) управление конфигурациями объектов информатизации;

в) управление уязвимостями и обновлениями (исправлениями) объектов информатизации.

Примечание — Управление конфигурациями, уязвимостями и обновлениями (исправлениями) предусмотрено в отношении объектов информатизации, входящих в критичную архитектуру.

При реализации процесса «Управление изменениями» рекомендуется использовать положения ГОСТ Р 56545 (см. также [23]—[25]).

7.3.2 Состав мер по организации и выполнению процедур управления изменениями в критичной архитектуре применительно к уровням защиты приведен в таблице 2.

Таблица 2

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.1	Планирование, информирование вовлеченных подразделений о вносимых изменениях и контроль внесения изменений в критичную архитектуру	О	Т	Т
УИ.2	Классификация в целях приоритизации изменений (например, плановые, срочные и критичные изменения) в критичную архитектуру	О	О	О
УИ.3	Выявление, оценка и утверждение срочных и критичных изменений	О	О	О
УИ.4	Привлечение службы ИБ, а также при необходимости иных подразделений, формирующих «вторую линию защиты», в рамках процесса управления изменениями: - для выявления и идентификации риска реализации информационных угроз; - участия в разработке мероприятий, направленных на уменьшение негативного влияния от выявленного и идентифицированного риска реализации информационных угроз; - контроля за реализацией мероприятий, направленных на уменьшение негативного влияния от выявленного и идентифицированного риска реализации информационных угроз	Н	О	О
УИ.5	Реализация механизма согласования (в том числе со стороны службы ИБ, а также подразделения, ответственного за организацию управления операционным риском*) и утверждения внесения изменений в критичную архитектуру, в том числе назначение должностных лиц, ответственных за рассмотрение и утверждение предлагаемых изменений	О	О	О
УИ.6	Реализация формализованных процедур анализа вносимых изменений в критичную архитектуру в части:			
УИ.6.1	- контроля соответствия заявленным целям внесения изменений	О	О	О
УИ.6.2	- контроля требований безопасности вносимых изменений	О	О	О
УИ.6.3	- реализации отдельных сред разработки, тестирования и постоянной эксплуатации, включая контроль переноса и целостности информации (данных) при переносе между указанными средами	Н	Т	Т
УИ.6.4	- контроля отсутствия известных (описанных) уязвимостей объектов информатизации	О	Т	Т
УИ.7	Реализация механизма последующего контроля внесенных изменений в критичную архитектуру, в том числе в части соблюдения установленных требований к процессу внесения изменений	О	О	О
УИ.8	Определение субъектов доступа, обладающих полномочиями для внесения изменений в критичную архитектуру в целях предоставления соответствующих прав доступа к объектам информатизации	О	О	Т
УИ.9	Фиксация и протоколирование внесенных изменений в критичную архитектуру	Н	О	Т
УИ.10	Реализация механизма возврата к исходным условиям функционирования, в том числе если внесенные изменения негативно повлияли на уровень риска реализации информационных угроз и (или) обеспечение операционной надежности	Т	Т	Т

Окончание таблицы 2

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.11	Интеграция процесса управления изменениями с процессом идентификации критичной архитектуры, включая:			
УИ.11.1	- внесение изменений в критичную архитектуру с учетом оценки риска реализации информационных угроз (включая остаточный риск) и влияния на операционную надежность финансовой организации до и после внесения изменений	О	О	О
УИ.11.2	- обновление инвентарных данных о критичных активах (элементах критичной архитектуры) при внесении изменений в критичную архитектуру, в том числе для фиксации фактов внедрения новых, перемещения и (или) перепрофилирования существующих, а также выявления неучтенных объектов информатизации	Н	О	Т
УИ.11.3	- обновление данных об используемых сервисах поставщиков облачных услуг и применяемых мерах защиты информации для таких сервисов	Н	О	Т
УИ.12	Проведение анализа на предмет необходимости переоценки риска реализации информационных угроз** перед внесением изменений в критичную архитектуру финансовой организации, включая выявление фактов***, свидетельствующих о возможном изменении уровня такого риска	Н	О	О

* Если требования нормативных актов Банка России не устанавливают обязанность финансовой организации создания соответствующего подразделения, в целях реализации механизма согласования следует привлекать службу управления рисками.

** В случае выявления необходимости переоценки риска реализации информационных угроз, по результатам такой переоценки финансовым организациям следует разработать мероприятия, направленные на снижение негативного влияния риска реализации информационных угроз перед внесением изменений в критичную архитектуру.

*** Например, выявление новых информационных угроз (и связанных с ними уязвимостей), неблагоприятные результаты анализа вносимых изменений, изменение или смена аппаратного, программного и (или) аппаратно-программного обеспечения, в том числе изменение конфигураций объектов информатизации.

7.3.3 Состав мер по управлению конфигурациями объектов информатизации (входящих в критичную архитектуру) применительно к уровням защиты приведен в таблице 3.

Таблица 3

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.13	Определение области применения процесса управления изменениями в части управления конфигурациями, включающей определение: - настраиваемых объектов информатизации* и устанавливаемых настроек**; - настраиваемых функций, портов, протоколов (включая протоколы удаленного доступа), служб (сервисов) для настраиваемых объектов информатизации; - состава ПО (в том числе прикладного ПО и приложений) на автоматизированных рабочих местах работников финансовой организации; - объектов информатизации, для которых невозможно обеспечить централизованную установку, применение и контроль внутренних стандартов конфигурирования объектов информатизации (стандартов конфигурирования); - состава используемых сервисов поставщиков облачных услуг (в случае наличия возможности определить состав таких сервисов)	О	О	О

Продолжение таблицы 3

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.14	Идентификация и поддержание в актуальном состоянии инвентарных данных о составе и конфигурациях объектов информатизации***	О	О	Т
УИ.15	Определение процедур по установлению, применению и контролю стандартов конфигурирования, определяющих заданный уровень и необходимые политики (режимы) защиты информации	О	О	О
УИ.16	Включение в состав процедур по установлению, применению и контролю стандартов конфигурирования:			
УИ.16.1	- централизованная*4 установка, применение и контроль (в том числе с применением средств автоматизации) стандартов конфигурирования	Н	О	Т
УИ.16.2	- включение в состав стандартов конфигурирования условий функционирования объекта информатизации*5	О	О	О
УИ.16.3	- обеспечение соответствия стандартов конфигурирования текущей критичной архитектуре, установление и выполнение правил обновления (актуализации) стандартов конфигурирования	О	О	О
УИ.16.4	- хранение предыдущих версий стандартов конфигурирования и обеспечение возможности возврата к ним	Т	Т	Т
УИ.16.5	- раздельное управление стандартами конфигурирования (в том числе их раздельное использование) для сред разработки, тестирования и постоянной эксплуатации	Н	Т	Т
УИ.16.6	- разграничение доступа и контроль несанкционированного изменения стандартов конфигурирования	О	Т	Т
УИ.16.7	- согласование (в том числе со стороны службы ИБ) и утверждение внесения изменений в стандарты конфигурирования	О	Т	Т
УИ.17	Привлечение службы ИБ в рамках процесса управления изменениями в части управления конфигурациями, включая согласование стандартов конфигурирования	О	О	О
УИ.18	Проведение регулярного контроля соответствия текущих конфигураций объектов информатизации стандартам конфигурирования, включая контроль со стороны службы ИБ, в целях:			
УИ.18.1	- контроля и выявления несанкционированного изменения текущих конфигураций объектов информатизации, а также их несоответствия стандартам конфигурирования	О	Т	Т
УИ.18.2	- реагирования в случаях выявления несанкционированного изменения текущих конфигураций объектов информатизации	О	О	О
УИ.19	Применение для обеспечения безопасности конфигурирования объектов информатизации международных и отечественных практик, в том числе для проведения анализа безопасности применяемых (или планируемых к применению) конфигураций объектов информатизации	О	О	О
УИ.20	Разработка планов управления конфигурациями*6 на первоначальных этапах жизненного цикла (разработка или приобретение) объектов информатизации, входящих в критичную архитектуру	Н	О	О
УИ.21	Управление конфигурациями объектов информатизации на этапах жизненного цикла, связанных с установкой (внедрением), обновлением (модификацией) и удалением (уничтожением) объектов информатизации	Н	О	О

Окончание таблицы 3

* К объектам информатизации, включенным в область применения процесса управления изменениями в части управления конфигурациями, следует относить входящие в состав критичной архитектуры объекты информатизации, такие как: - автоматизированные рабочие места работников финансовой организации [включая переносные (мобильные) устройства]; - серверы (управления базами данных, почтовые, аутентификационные, веб-серверы, прокси-серверы, файловые, доменные); - устройства ввода/вывода (сканеры, копиры, принтеры, многофункциональные устройства); - сетевые устройства [межсетевые экраны, маршрутизаторы, сетевые шлюзы, сетевые коммутаторы, беспроводные точки доступа, сетевые программно-аппаратные комплексы, датчики (сенсоры, агенты), подключенные к сети]; - объекты информатизации, находящиеся под управлением поставщика облачных услуг (в случае наличия возможности определить состав таких сервисов). ** К устанавливаемым настройкам объектов информатизации в том числе относятся параметры безопасности, такие как настройки: - системного реестра операционной системы; - разрешений и полномочий (в отношении учетных записей, отдельных файлов и директорий); - в отношении функций, портов, протоколов, служб (сервисов) и процедур удаленного доступа. *** Реализуется совместно с процессом «Идентификация критичной архитектуры» и процессом «Контроль целостности и защищенности информационной инфраструктуры», базовый состав организационных и технических мер в рамках которого определен ГОСТ Р 57580.1. *4 В случае невозможности централизованной установки, применения и контроля стандартов конфигурирования финансовой организации это следует отразить при определении области применения процесса управления изменениями в части управления конфигурациями. *5 К таким условиям функционирования объекта информатизации следует, как минимум, относить: - исходный состав (пакеты) ПО, устанавливаемого на объекты информатизации, с указанием версии и примененных обновлений (исправлений); - примененные в отношении объекта информатизации настройки; - сетевое расположение объекта информатизации; - взаимосвязи объекта информатизации (топологию взаимосвязей) в рамках вычислительной сети (сегмента вычислительной сети), в которой он расположен. *6 В частности, планы должны описывать: - процедуры управления конфигурациями объектов информатизации, в том числе в зависимости от среды (разработки, тестирования и эксплуатации); - обновление настроек конфигураций; - разработку, выпуск и обновление документации на объект информатизации.

7.3.4 Состав мер по управлению уязвимостями и обновлениями (исправлениями) объектов информатизации, входящих в критичную архитектуру, применительно к уровням защиты приведен в таблице 4.

Таблица 4

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.22	Определение, выполнение и контроль процедур* по выявлению, приоритизации, классификации, устранению, а также контролю полноты и своевременности устранения выявленных уязвимостей в критичной архитектуре, присущих:			
УИ.22.1	- реализации бизнес- и технологических процессов	Н	О	О
УИ.22.2	- объектам информатизации прикладного уровня	Н	О	О
УИ.22.3	- объектам информатизации инфраструктурного уровня	О	О	О
УИ.23	Включение в состав процедур, предусмотренных мерой УИ.22, в отношении объектов информатизации инфраструктурного уровня:			
УИ.23.1	- поддержание актуальности данных о доступных обновлениях (исправлениях) для устранения уязвимостей	О	О	О

Продолжение таблицы 4

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.23.2	- выявление необходимости применения соответствующих обновлений (исправлений) для отдельных объектов информатизации и проведение анализа безопасности их применения	О	О	О
УИ.23.3	- обеспечение корректного применения обновлений (исправлений), включая предварительный и последующий контроль их применения (например, согласно принципу «четырех глаз»)	Н	О	Т
УИ.23.4	- документарное определение процедур, связанных с применением обновлений (исправлений)	Н	Н	О
УИ.24	Применение инструментов и (или) способов выявления уязвимостей объектов информатизации, входящих в критичную архитектуру, обеспечивающих в том числе:			
УИ.24.1	- выявление вредоносного кода	Т	Т	Т
УИ.24.2	- выявление неконтролируемого использования технологии мобильного кода**	Н	Т	Т
УИ.24.3	- выявление неавторизованного логического доступа к ресурсам доступа, в том числе автоматизированным системам	Т	Т	Т
УИ.25	Управление обновлениями (исправлениями) объектов информатизации в рамках процесса управления изменениями, включая:			
УИ.25.1	- рассмотрение возможности применения соответствующих стандартов конфигурирования при применении обновлений (исправлений) объектов информатизации, входящих в критичную архитектуру	О	О	О
УИ.25.2	- реализации процедур предварительного анализа*** и согласования применения обновлений (исправлений)	О	О	Т
УИ.25.3	- реализации процедур запрета применения обновлений (исправлений), которые предварительно не согласованы	О	О	Т*4
УИ.25.4	- реализации процедур быстрого восстановления выполнения бизнес- и технологических процессов (в том числе возврата к исходным условиям функционирования объектов информатизации) в случае неудачного применения обновлений (исправлений)*5	О	Т	Т
УИ.25.5	- применение отдельных сред разработки, тестирования и постоянной эксплуатации, обеспечивающих возможность быстрого тестирования	Н	Т	Т
УИ.25.5	(проверки) обновлений (исправлений), а также при необходимости быстрого восстановления выполнения бизнес- и технологических процессов (возврата к исходным условиям функционирования объектов информатизации)	Н	Н	О
УИ.25.6	- анализа и применения передового опыта (в том числе по использованию средств автоматизации) в целях устранения технических и организационных недостатков, а также обеспечения контроля соответствия установленным стандартам конфигурирования и политикам (режимам) защиты информации	Н	Н	О
УИ.25.7	- контроль соответствия примененных (установленных) обновлений (исправлений) объектов информатизации наиболее актуальным (новейшим) версиям обновлений (исправлений)	О	О	Т
УИ.25.8	- контроль своевременности применения (установки) обновлений (исправлений) объектов информатизации	О	О	О

Продолжение таблицы 4

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.26	Управление уязвимостями на этапах жизненного цикла разработки объектов информатизации прикладного уровня (прикладного ПО), включая применение инструментов анализа (инспекции) кода (code review), посредством статического и динамического тестирования	Н	О	О
УИ.27	Регулярный[*6] анализ уязвимостей (сканирование на уязвимости) объектов информатизации инфраструктурного уровня, в том числе сканирование на уязвимости: - объектов информатизации, непосредственно взаимодействующих с сетью Интернет; - «внутренних» объектов информатизации, в том числе вычислительных сетей, на «границах» контуров безопасности	Н	О	О
УИ.28	Регулярное[*7] тестирование на проникновение (симуляция компьютерных атак), в том числе тестирование на проникновение: - объектов информатизации, непосредственно взаимодействующих с сетью Интернет; - «внутренних» объектов информатизации, в том числе вычислительных сетей, на «границах» контуров безопасности	Н	О	О
УИ.29	Применение риск-ориентированного подхода к выбору объектов информатизации, подвергаемых тестированию на проникновение, в том числе в части периодичности проведения тестирования на проникновение	Н	О	О
УИ.30	Проведение сканирования на уязвимости и (или) тестирование на проникновение при существенных изменениях в критичной архитектуре и (или) внедрении новых объектов информатизации (автоматизированных систем)	Н	О	О
УИ.31	Проведение анализа системных журналов для выявления фактов эксплуатации в прошлом уязвимостей, аналогичных вновь выявленным	Н	Н	О
УИ.32	Тестирование «red team», т. е. симуляция действий нарушителя безопасности в контролируемых условиях, в том числе для симуляции попыток реализации компьютерных атак в отношении объектов информатизации, входящих в критичную архитектуру, в соответствии с заранее определенными сценариями	Н	Н	О
УИ.33	Использование в качестве источников информации об уязвимостях, а также регулярное обновление и контроль актуальности используемой информации для проведения сканирования на уязвимости: - баз данных общеизвестных уязвимостей (например, [26], [27]); - сведений об уязвимостях, полученных в рамках тестирования «red team»; - иных источников	О	О	О
УИ.34	Организация тестирования «red team» в отношении критичной архитектуры для оценки возможных уязвимостей, в том числе в процессах обеспечения операционной надежности и защиты информации, согласно следующим принципам: - применения надежных и ценных сведений об информационных угрозах (в том числе компьютерных атаках), полученных в рамках исследования (разведки) потенциальных угроз и основанных на актуальных и вероятных сценариях реализации таких угроз (в том числе компьютерных атак); - обеспечения независимости и компетентности команды, привлекаемой к тестированию «red team»	Н	Н	О

Окончание таблицы 4

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
УИ.35	Ведение реестра выявленных и устраненных уязвимостей[*8], в том числе фиксация совершенных действий по устранению уязвимостей	О	Т	Т
УИ.36	Оценка эффективности[*9] деятельности по управлению уязвимостями (как минимум с учетом времени, затрачиваемого на устранение уязвимостей с момента их выявления)	Н	О	О
УИ.37	Организация мониторинга статуса работ по устранению уязвимостей	Н	Т	Т

[*] Включая определение применяемых инструментов и (или) способов выявления уязвимостей.

[**] В том числе Java, JavaScript, ActiveX, VBScript и иные аналогичные технологии.

[***] Предварительный анализ может включать:

- анализ влияния обновлений (исправлений) на взаимосвязанные объекты информатизации и (или) их компоненты;
- проверку работоспособности объектов информатизации после применения обновлений (исправлений) в среде тестирования;
- определение действий в отношении обновлений (исправлений), проверка работоспособности в отношении которых прошла неуспешно.

[*4] При невозможности технической реализации указанной меры путем применения технической меры [например, в отношении проприетарного ПО, обновление которого осуществляется посредством автоматизированных инструментов, предоставляемых разработчиком (поставщиком) такого ПО] рекомендуется рассматривать в качестве компенсирующих мер, направленных на предотвращение неконтролируемого применения обновлений (исправлений) объектов информатизации прикладного уровня, например применение автоматизированных инструментов последующего контроля соответствия запланированных и примененных обновлений (исправлений).

[*5] Для обновлений (исправлений), применяемых в рамках среды постоянной эксплуатации, должен быть разработан план восстановления выполнения бизнес- и технологических процессов (возврата к исходным условиям функционирования объектов информатизации или использования резервных ресурсов, или применения альтернативных способов выполнения бизнес- и технологических процессов) в случае неудачного применения обновлений (исправлений).

[*6] В случае выявления и (или) получения информации об уязвимостях, обладающих потенциалом негативного влияния на объекты информатизации финансовой организации, проводят внеплановое сканирование уязвимостей или ручную проверку при наличии информации о механизме эксплуатации уязвимости/«проверки концепции» (proof of concept).

[*7] В случае внедрения изменений и (или) применения значительных обновлений (исправлений) объектов информатизации, непосредственно взаимодействующих с сетью Интернет, проводят их внеплановое тестирование на проникновение.

[*8] Финансовым организациям следует рассмотреть возможность использования инструментов для работы в рамках Общей системы оценки уязвимостей (Common Vulnerability Scoring System).

[*9] Оценку эффективности деятельности по управлению уязвимостями следует осуществлять в рамках регулярной оценки эффективности системы управления риском реализации информационных угроз, меры по проведению которой предусмотрены ГОСТ Р 57580.3, в том числе согласно требованиям нормативных актов Банка России [6].

7.4 Процесс 3 «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации»

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

- выявление и фиксацию инцидентов, в том числе обнаружение компьютерных атак и выявление фактов (индикаторов) компрометации объектов информатизации;
- реагирование на инциденты в отношении критичной архитектуры;
- восстановление функционирования бизнес- и технологических процессов и 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 их реализации.

При реализации процесса «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации» рекомендуется использовать [28]—[31].

7.4.2 Состав мер по выявлению и фиксации инцидентов, в том числе обнаружению компьютерных атак и выявлению фактов (индикаторов) компрометации объектов информатизации применительно к уровням защиты, приведен в таблице 5.

Таблица 5

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.1	Организация мониторинга и выявления событий, связанных с возможной реализацией информационных угроз в рамках процессов, реализуемых в соответствии с требованиями ГОСТ Р 57580.1, в целях своевременного обнаружения: - компьютерных атак; - аномальной активности лиц, имеющих легальный доступ к объектам информатизации финансовой организации; - неправомерного использования доступа поставщиками услуг или другими доверенными организациями; - фактов утечки защищаемой информации	О	О	О
ВРВ.2	Организация мониторинга и выявления событий реализации информационных угроз, предусмотренных мерой ВРВ.1, с учетом технического описания сценариев возможных компьютерных атак*	Н	О	О
ВРВ.3	Организация сбора и фиксации технических данных (свидетельств)** о выявленных событиях реализации информационных угроз в рамках процессов защиты информации, реализуемых в соответствии с ГОСТ Р 57580.1, в целях проведения их последующего анализа, а также в случае необходимости проведения компьютерной экспертизы	Н	О	О
ВРВ.4	Создание механизмов инициативного информирования работниками финансовой организации о событиях реализации информационных угроз, в частности реализации компьютерных атак	О	О	Т
ВРВ.5	Организация и выполнение деятельности по получению сведений об актуальных индикаторах компрометации объектов информатизации: - от Банка России, осуществляющего направление таких сведений в соответствии с требованиями законодательства Российской Федерации [2]; - доверенных причастных сторон, осуществляющих направление таких сведений	Т	Т	Т
ВРВ.6	Реализация защиты от вредоносного кода на основе полученных сведений об актуальных индикаторах компрометации объектов информатизации, в том числе с привлечением для выполнения такой деятельности специалистов, обладающих необходимой компетенцией***	Т	Т	Т

* В указанном случае мониторинг событий реализации информационных угроз целесообразно выстраивать согласно принципу эшелонированной защиты, подбирая индивидуальный набор инструментов мониторинга для каждого отдельного контура безопасности в зависимости:

- от наличия в рамках рассматриваемого контура безопасности объектов информатизации, отвечающих критериям доступности из внешней сети Интернет;
- состава бизнес- и технологических процессов, реализуемых в рамках рассматриваемого контура безопасности;
- класса защищаемой информации, хранимой, подготавливаемой и передаваемой в рамках рассматриваемого контура безопасности.

Окончание таблицы 5

** Рекомендуется определять набор и объем собираемых технических данных (свидетельств) таким образом, чтобы обеспечивалась возможность выявления и детального описания новых информационных угроз, включая ранее неизвестные уязвимости и сценарии реализации таких угроз. Набор и объем собираемых технических данных (свидетельств) также следует рассматривать на предмет достаточности для случаев регистрации произошедших инцидентов в качестве событий риска реализации информационных угроз в базе событий риска согласно требованиям нормативных актов Банка России, в частности [6].

Организацию и выполнение деятельности по сбору и фиксации технических данных (свидетельств) целесообразно осуществлять с учетом рекомендаций, приведенных в [32].

*** Если финансовая организация не располагает необходимыми компетенциями, рекомендуется рассмотреть возможность заключения договоров (контрактов) с поставщиками соответствующих услуг.

7.4.3 Состав мер по реагированию на инциденты в отношении критичной архитектуры применительно к уровням защиты приведен в таблице 6.

Таблица 6

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.7	Определение порядка реагирования на инциденты, включая разработку и определение:			
ВРВ.7.1	- целевых показателей реагирования на инциденты	О	О	О
ВРВ.7.2	- методологии проведения предварительной оценки потенциала влияния (критичности) инцидента, включая его классификацию согласно типовому перечню и классификационным признакам	Н	О	О
ВРВ.7.3	- типового перечня инцидентов и классификационных признаков, в том числе на основе классификатора событий риска реализации информационных угроз согласно приложениям А, Б, В, Г ГОСТ Р 57580.3—2022	О	О	О
ВРВ.7.4	- ролей, связанных с реагированием на инциденты	О	О	О
ВРВ.7.5	- правил и процедур (playbooks) реагирования на инциденты	О	О	О
ВРВ.7.6	- перечня причастных сторон (за исключением клиентов финансовой организации), с которыми финансовая организация осуществляет взаимодействие в рамках реагирования на инциденты	О	О	О
ВРВ.7.7	- форматов и способов реализации информационного обмена об инцидентах внутри финансовой организации, а также с причастными сторонами в рамках реагирования на инциденты	О	О	О
ВРВ.7.8	- показателей оценки эффективности реагирования на инциденты, характеризующих степень достижения установленных целевых показателей	О	О	О
ВРВ.8	Утверждение порядка реагирования на инциденты единоличным исполнительным органом финансовой организации или должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз финансовой организации	О	О	О
ВРВ.9	Определение в качестве целевых показателей реагирования на инциденты: - ограничение распространения и предотвращение повторения инцидентов внутри финансовой организации, а также среди причастных сторон, в том числе клиентов финансовой организации; - ограничение СТП инцидентов для финансовой организации для соблюдения контрольных и сигнальных значений КПУР, предусмотренных ГОСТ Р 57580.3, в том числе ограничение собственных финансовых потерь, а также финансовых потерь причастных сторон, включая клиентов финансовой организации;	О	О	О

Продолжение таблицы 6

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.9	- соблюдение допустимого времени простоя и (или) деградации бизнес- и технологических процессов, а также сигнальных и контрольных значений КПУР, предусмотренных ГОСТ Р 57580.3, с учетом требований нормативных актов Банка России [6]—[8]	О	О	О
ВРВ.10	Включение в состав классификационных признаков инцидентов, как минимум: - типы компьютерных атак; - векторы (направления) компьютерных атак; - типы атакуемых объектов; - тип нарушителя безопасности информации; - бизнес- и технологические процессы (включая технологические участки), в рамках которых реализована или может быть реализована компьютерная атака; - возможные последствия, в том числе финансовых потерь от реализации инцидентов	Н	О	О
ВРВ.11	Организация и выполнение деятельности по проведению предварительной оценки потенциала влияния (критичности) инцидента, включая его классификацию согласно типовому перечню и классификационным признакам* в целях:			
ВРВ.11.1	- применения соответствующего набора правил и процедур (playbooks) реагирования на инциденты, утверждаемого должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз	Н	О	О
ВРВ.11.2	- информирования причастных сторон (включая клиентов финансовой организации, в случае возникновения такой необходимости), на которых повлияли или могут повлиять последствия инцидента	О	О	О
ВРВ.11.3	- информирования Банка России и федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в соответствии с требованиями законодательства Российской Федерации [5], в том числе нормативных актов Банка России [7], [8], [11]—[13], [33]	Н	О	О
ВРВ.12	Включение в состав ролей в рамках реагирования на инциденты в дополнение к ролям группы реагирования на инциденты защиты информации (ГРИЗИ), предусмотренным ГОСТ Р 57580.1:			
ВРВ.12.1	- роли владельца инцидента (подразделения, в рамках деятельности которого произошел инцидент), ответственного за координацию своей деятельности в условиях реализации отдельного инцидента	Н	О	О
ВРВ.12.2	- роли независимого наблюдателя, ответственного за фиксацию (документирование) действий, предпринятых в рамках реагирования на каждом этапе реализации отдельного инцидента	Н	О	О
ВРВ.12.3	- роли ответственного за взаимодействие с общественностью и средствами массовой информации (СМИ), агрегирующего информацию о статусе обработки инцидентов для упорядоченного обновления и направления информационных сообщений для общественности и СМИ	Н	Н	О

Продолжение таблицы 6

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.13	Разработка** состава правил и процедур (playbooks) реагирования на инциденты на основе: - информации, полученной в рамках консультации с подразделениями, формирующими «первую линию защиты» (пример распределения подразделений финансовой организации согласно принципу «трех линий защиты» приведен в ГОСТ Р 57580.3); - возможных сценариев реализации информационных угроз (в том числе компьютерных атак); - сценариев реализовавшихся информационных угроз (в том числе компьютерных атак)	О	О	О
ВРВ.14	Включение в состав правил и процедур (playbooks) реагирования на инциденты, в том числе процедур:			
ВРВ.14.1	- приоритизации, эскалации и принятия (или делегирования прав по принятию) решений в рамках реагирования на инциденты, в том числе на основе определенного уровня критичности инцидента	Н	Т	Т
ВРВ.14.2	- взаимодействия финансовой организации с Банком России, причастными сторонами, в том числе с клиентами финансовой организации, в целях ограничения финансовых потерь от осуществления финансовых (банковских) операций, в том числе переводов денежных средств, без согласия клиента	О	Т	Т
ВРВ.14.3	- взаимодействия финансовой организации с общественностью и СМИ при реализации инцидентов	Н	О	О
ВРВ.14.4	- по ограничению распространения инцидентов	О	О	О
ВРВ.14.5	- по снижению СТП инцидентов	О	О	О
ВРВ.14.6	- сбора и фиксации технических данных (свидетельств) в рамках реагирования на инциденты для анализа причин и последствий реализации инцидентов	Н	О	Т
ВРВ.14.7	- формирования отчетности в рамках реагирования на инциденты, в том числе в целях реализации требований нормативных актов Банка России, в частности [6]	О	О	Т
ВРВ.15	Организация и выполнение деятельности в рамках реагирования на инциденты согласно установленным правилам и процедурам (playbooks) в зависимости от уровня влияния (критичности) инцидента	О	О	О
ВРВ.16	Организация и выполнение деятельности по ограничению распространения инцидентов внутри финансовой организации, а также среди причастных сторон (за исключением клиентов финансовой организации), в том числе:			
ВРВ.16.1	- оперативное устранение или ограничение воздействия источников и причин реализации инцидентов	О	О	Т
ВРВ.16.2	- изоляция или отключение объектов информатизации (части объектов информатизации), на которые повлияла или может повлиять реализация инцидента***	О	О	Т
ВРВ.17	Организация и выполнение деятельности по снижению тяжести последствий от реализации инцидентов, в том числе:			
ВРВ.17.1	- сдерживание и (или) предотвращение реализации компьютерных атак и их последовательностей, в том числе на разных уровнях информационной инфраструктуры, с учетом технического описания сценариев возможных компьютерных атак	Н	О	Т

Окончание таблицы 6

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.17.2	- применение риск-ориентированной модели для установления лимитов по параметрам финансовых (банковских) операций, в том числе переводов денежных средств, при использовании каналов дистанционного обслуживания	Н	О	Т
ВРВ.17.3	- реализация механизмов приостановления осуществления финансовых (банковских) операций, в том числе операций по переводу денежных средств, в соответствии с нормативными актами Банка России [34]	Н	О	Т
ВРВ.18	Организация и выполнение деятельности по сбору и фиксации технических данных (свидетельств)*4 в рамках реагирования на инциденты, в том числе во взаимодействии с причастными сторонами, способом, обеспечивающим юридическую значимость собранных данных	Н	Т	Т
ВРВ.19	Обеспечение возможности проведения компьютерной экспертизы в целях сбора и фиксации технических данных (свидетельств), в том числе посредством заключения контрактов (договоров) с поставщиками услуг в том случае, если финансовая организация не располагает необходимыми для данной деятельности компетенциями	Н	Н	О
ВРВ.20	Уничтожение всех вредоносных элементов (артефактов) с объектов информатизации, в отношении которых реализовался инцидент, после сбора и фиксации технических данных (свидетельств)	Т	Т	Т

* Для проведения предварительной оценки потенциала влияния (критичности) инцидента финансовой организацией должны быть заранее определены шкала критичности инцидентов и критерии отнесения инцидентов к различным уровням согласно данной шкале. Результатом такой оценки является присвоение уровня критичности инциденту согласно заранее определенной шкале.

** Для проработки или проверки отдельных норм (в том числе технического характера), требующих высокой квалификации исполнителя, в рамках разработки правил и процедур (playbooks) реагирования на инциденты финансовым организациям следует привлекать внутренних или внешних экспертов.

*** При принятии решений об изоляции или отключении объектов информатизации (части объектов информатизации), на которые повлияла или может повлиять реализация инцидента, финансовым организациям следует учитывать влияние таких действий:

- на осуществление видов деятельности финансовой организации;
- уровень операционного риска;
- затраты и потери финансовой организации.

*4 Организацию и выполнение деятельности по сбору и фиксации технических данных (свидетельств) целесообразно осуществлять с учетом рекомендаций, приведенных в [32].

7.4.4 Состав мер по восстановлению функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов применительно к уровням защиты приведен в таблице 7.

Таблица 7

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.21	Определение порядка восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов, включая разработку и определение:			
ВРВ.21.1	- целевых показателей восстановления после реализации инцидентов	О	О	О
ВРВ.21.2	- ролей, связанных с восстановлением после реализации инцидентов	О	О	О
ВРВ.21.3	- правил и процедур (playbooks) восстановления после реализации инцидентов	Н	О	О

Продолжение таблицы 7

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.21.4	- перечня причастных сторон (за исключением клиентов финансовой организации), с которыми финансовая организация осуществляет взаимодействие в рамках восстановления после реализации инцидентов	О	О	О
ВРВ.21.5	- форматов и способов реализации информационного обмена о предпринятых действиях и статусе восстановления после инцидентов внутри финансовой организации, а также с причастными сторонами в рамках восстановления после реализации инцидентов	О	О	О
ВРВ.21.6	- критериев оценки завершения восстановления и условий закрытия инцидента	О	О	О
ВРВ.21.7	- показателей оценки эффективности восстановления после реализации инцидентов	О	О	О
ВРВ.22	Утверждение порядка восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов единоличным исполнительным органом финансовой организации или должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз финансовой организации	О	О	О
ВРВ.23	Определение в качестве целевых показателей восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов: - выявление и устранение причин реализации инцидентов; - восстановление функционирования бизнес- и технологических процессов и объектов информатизации, а также восстановление данных финансовой организации в соответствии с заданными объемами (ЦТВД) и временными периодами (ЦВВ), устанавливаемыми с учетом допустимого уровня простоя и (или) деградации бизнес- и технологических процессов, а также сигнальных и контрольных значений КПУР, предусмотренных ГОСТ Р 57580.3	О	О	О
ВРВ.24	Определение ролей, связанных с восстановлением функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов, и привлечение к их выполнению, в том числе: - работников службы информационной безопасности; - работников подразделения информатизации, ответственных за поддержание функционирования объектов информатизации; - работников подразделений, формирующих «первую линию защиты»; - работников иных подразделений, формирующих «вторую линию защиты», в случае необходимости; - внешних экспертов, посредством заключения соответствующих контрактов (договоров) в том случае, если финансовая организация не располагает необходимыми для данной деятельности компетенциями среди собственных работников	О	О	О
ВРВ.25	Разработка (а также утверждение должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз) состава правил и процедур (playbooks) восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов на основе: - информации, полученной в рамках консультации с владельцами бизнес-процессов финансовой организации; - условий функционирования объектов информатизации; - сценариев реализовавшихся информационных угроз	О	О	О

Продолжение таблицы 7

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.26	Включение в состав правил и процедур (playbooks) восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов:			
ВРВ.26.1	- процедур выявления и устранения причин реализации инцидентов, в том числе путем обновления состава объектов информатизации финансовой организации	О	О	О
ВРВ.26.2	- процедур восстановления выполнения бизнес- и технологических процессов финансовой организации в заданные временные периоды (согласно ЦВВ)	О	О	О
ВРВ.26.3	- процедур восстановления функционирования объектов информатизации на каждом из уровней информационной инфраструктуры с учетом взаимосвязей и взаимозависимостей между объектами информатизации	О	О	О
ВРВ.26.4	- процедур восстановления данных* с помощью резервных копий в заданных объемах (согласно ЦТВД)	Т	Т	Т
ВРВ.26.5	- процедур привлечения, в случае необходимости, компетентных специалистов соответствующих организаций — поставщиков услуг	О	О	О
ВРВ.26.6	- процедур по снижению СТП инцидентов	О	О	О
ВРВ.26.7	- процедур сбора и фиксации технических данных (свидетельств) в рамках восстановления после реализации инцидентов для анализа причин и последствий реализации инцидентов	Н	Т	Т
ВРВ.26.8	- процедур формирования отчетности в рамках восстановления после реализации инцидентов	О	О	Т
ВРВ.26.9	- графика (приоритетности и последовательности) при восстановлении функционирования бизнес- и технологических процессов и объектов информатизации	О	О	О
ВРВ.27	Организация и выполнение деятельности в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов согласно утвержденным** правилам и процедурам (playbooks)	О	О	О
ВРВ.28	Регистрация (документирование) выполняемых действий (операций)*** (а также фиксация времени начала и окончания их выполнения) в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов согласно утвержденным правилам и процедурам (playbooks)	Н	О	Т
ВРВ.29	Организация и выполнение деятельности по снижению СТП инцидентов, в том числе:			
ВРВ.29.1	- обеспечение непрерывности выполнения бизнес- и технологических процессов за счет использования резервных (альтернативных) каналов (способов) предоставления финансовых и (или) информационных услуг и объектов информатизации	О	О	О
ВРВ.29.2	- обеспечение возможности перехода от эксплуатации основных каналов (способов) предоставления финансовых и (или) информационных услуг и объектов информатизации к резервным (альтернативным) в соответствии с заданными временными периодами (ЦВВ) и заданными объемами восстановления данных (ЦТВД)	О	Т	Т

Окончание таблицы 7

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.30	Определение в качестве критериев для оценки завершения восстановления функционирования бизнес- и технологических процессов и объектов информатизации и условий закрытия инцидента, в том числе: - проведение тестирования (проверки)*4 восстановленных бизнес- и технологических процессов, объектов информатизации и данных; - полное устранение или нейтрализация воздействия источника реализовавшегося инцидента	О	О	О
ВРВ.31	Организация и выполнение деятельности по проведению оценки завершения восстановления функционирования бизнес- и технологических процессов и объектов информатизации согласно определенным критериям перед принятием решения о закрытии соответствующего инцидента	О	О	О
ВРВ.32	Организация и выполнение деятельности по сбору и фиксации технических данных (свидетельств)*5 в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов, в том числе во взаимодействии с причастными сторонами, способом, обеспечивающим юридическую значимость собранных технических данных (свидетельств)	Н	Т	Т
ВРВ.33	Обеспечение возможности проведения компьютерной экспертизы в целях сбора и фиксации технических данных (свидетельств), в том числе посредством заключения контрактов (договоров) с поставщиками услуг в том случае, если финансовая организация не располагает необходимыми для данной деятельности компетенциями	Н	Н	О

* Процедуры восстановления данных должны разрабатываться и применяться с учетом требований, предъявляемых подразделениями, формирующими «первую линию защиты». Процедуры восстановления данных должны предусматривать возможность восстановления данных на стороне причастных сторон — участников финансовой экосистемы и поставщиков услуг. В отношении восстанавливаемых данных следует применять механизмы обеспечения целостности таких данных (сверки с данными из резервных центров хранения, проверки контрольных сумм). При наиболее неблагоприятном сценарии допускается восстановление данных финансовой организацией на основе сведений причастных сторон — участников финансовой экосистемы и поставщиков услуг, в том числе клиентов финансовой организации.

** В случае необходимости отклонения от утвержденных правил и процедур (playbooks) восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов такие отклонения проходят предварительную проверку и утверждаются должностным лицом, ответственным за функционирование системы управления риском реализации информационных угроз, до их внедрения.

*** Регистрация (документирование) операций, выполняемых в рамках восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидентов, включает описание примененных инструментов и внесенных в настройки объектов информатизации изменений в виде, позволяющем использовать этот опыт в будущем при решении подобных проблем.

*4 Перед возвращением объектов информатизации в режим штатного функционирования в производственной среде финансовым организациям следует провести соответствующие тесты на предмет:

- полного устранения вредоносных элементов (артефактов) от реализации инцидента, связанного с реализацией информационных угроз, в объектах информатизации;
- работоспособности объектов информатизации;
- соответствия настроек объектов информатизации установленным требованиям к безопасности.

*5 Организацию и выполнение деятельности по сбору и фиксации технических данных (свидетельств) целесообразно осуществлять с учетом рекомендаций, приведенных в [32].

7.4.5 Состав мер по проведению анализа причин и последствий реализации инцидентов применительно к уровням защиты приведен в таблице 8.

Таблица 8

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.34	Организация и выполнение деятельности по проведению анализа причин и последствий реализации инцидентов, включающего:			
ВРВ.34.1	- определение целевых показателей анализа технических данных (свидетельств)	Н	О	О
ВРВ.34.2	- сбор и анализ технических данных (свидетельств)* в рамках выявления, реагирования на инциденты и восстановления после их реализации	Н	Т	Т
ВРВ.34.3	- определение источников и выявление причин реализации инцидентов	О	Т	Т
ВРВ.34.4	- описание сценариев реализации инцидентов	Н	Н	О
ВРВ.34.5	- оценку последствий от реализации инцидентов, влияния последствий на КПУР, предусмотренных ГОСТ Р 57580.3, с учетом требований нормативных актов Банка России [6]—[8], в том числе оценку прямых и непрямых финансовых потерь от реализации инцидентов	О	О	О
ВРВ.34.6	- привлечение, при необходимости, к такому анализу Банка России (ФинЦЕРТ)**	О	О	О
ВРВ.34.7	- фиксацию и информирование о результатах проведенного анализа, в том числе в базе событий риска, предусмотренной ГОСТ Р 57580.3, с учетом требований нормативных актов Банка России [6]	О	О	О
ВРВ.34.8	- оценку эффективности*** выявления, реагирования на инциденты и восстановления после их реализации	О	О	О
ВРВ.35	Организация и выполнение деятельности по проведению компьютерной экспертизы в целях сбора и фиксации технических данных (свидетельств), в том числе посредством заключения контрактов (договоров) с поставщиками услуг, в том случае, если финансовая организация не располагает необходимыми для данной деятельности компетенциями среди собственных работников	Н	Н	О
ВРВ.36	Определение в качестве целевых показателей анализа технических данных (свидетельств), собранных в рамках выявления, реагирования на инциденты и восстановления после их реализации: - определение (в том числе выявление новых) сценариев реализации инцидентов; - предотвращение повторной реализации инцидентов; - проведение идентификации субъектов, реализующих инциденты; - своевременное выявление маркеров «скрытого» несанкционированного управления объектами информатизации	Н	О	О
ВРВ.37	Организация и выполнение деятельности по информированию о результатах проведенного анализа причин и последствий реализации инцидентов: - исполнительного органа финансовой организации*4; - должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз; - причастных сторон (за исключением клиентов финансовой организации); - Банка России (ФинЦЕРТ)*5	О	О	О
ВРВ.38	Определение в качестве показателей для оценки эффективности выявления, реагирования на инциденты и восстановления после их реализации: - оперативности выявления, регистрации и реагирования на инцидент;	О	О	О

Окончание таблицы 8

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.38	- своевременности и корректности предварительной оценки влияния (критичности) инцидента; - полноты, качества и оперативности восстановления функционирования бизнес- и технологических процессов и объектов информатизации после реализации инцидента; - эффективности выполнения процедур приоритизации, эскалации и принятия (или делегирования прав по принятию) решений; - эффективности взаимодействия в рамках реагирования на инциденты и восстановления после их реализации как внутри финансовой организации, так и с причастными сторонами, в том числе клиентами финансовой организации	О	О	О
[*] Организацию и выполнение деятельности по сбору и фиксации технических данных (свидетельств) целесообразно осуществлять с учетом рекомендаций, приведенных в [32]. [**] Финансовой организации следует определить условия привлечения к проведению анализа причин и последствий реализации инцидентов Банка России (ФинЦЕРТ). [***] Оценку эффективности деятельности по выявлению, реагированию на инциденты и восстановлению после их реализации следует осуществлять в рамках регулярной оценки эффективности системы управления риском реализации информационных угроз, меры по проведению которой предусмотрены ГОСТ Р 57580.3, в том числе согласно требованиям нормативных актов Банка России, в частности [6]. [*4] Финансовой организацией должны быть определены формат и условия информирования исполнительного органа финансовой организации о результатах проведенного анализа причин и последствий реализации инцидентов. [*5] Мера применяется в отношении тех инцидентов, о которых следует информировать Банк России на основании требований нормативных актов Банка России [7], [8], [11]—[13], [33] в соответствии с установленными формами и сроками [35].			

7.4.6 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 их реализации применительно к уровням защиты приведен в таблице 9.

Таблица 9

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.39	Организация и выполнение деятельности по информированию[*] об инцидентах Банка России и федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в соответствии с требованиями законодательства Российской Федерации [5], в том числе нормативных актов Банка России [7], [8], [11]—[13], [33]	О	Т	Т
ВРВ.40	Организация взаимодействия в целях координации действий по реагированию на инциденты и восстановлению после их реализации: - внутри финансовой организации (между структурными подразделениями, формирующими «три линии защиты»); - с причастными сторонами (за исключением клиентов финансовой организации), включая поставщиков услуг (в том числе поставщиков облачных услуг); - с Банком России (ФинЦЕРТ)	О	О	О

Продолжение таблицы 9

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.41	Организация и выполнение деятельности по информированию** согласно определенным форматам и способам информационного обмена в рамках реагирования на инциденты и восстановления после их реализации: - совета директоров (наблюдательного совета) финансовой организации и исполнительного органа финансовой организации; - должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз; - структурных подразделений, формирующих «три линии защиты» в рамках управления риском реализации информационных угроз; - причастных сторон, в том числе клиентов финансовой организации	О	О	О
ВРВ.42	Организация и выполнение деятельности по подготовке и направлению на рассмотрение совету директоров (наблюдательному совету) или коллегиальному исполнительному органу финансовой организации отчетов о реагировании на инциденты и восстановлении после их реализации не реже одного раза в год (в том числе согласно требованиям нормативного акта Банка России [6]), оказавших влияние на фактические значения КПУР, предусмотренные ГОСТ Р 57580.3 (с указанием информации, характеризующей влияние инцидентов на фактические значения КПУР) с учетом требований нормативных актов Банка России [6]—[8]	Н	О	О
ВРВ.43	Организация и выполнение деятельности по информированию должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз, по каждому факту реализации инцидентов: - о масштабах влияния реализации инцидента на осуществление видов деятельности финансовой организации, о влиянии на фактические значения КПУР, предусмотренные ГОСТ Р 57580.3, с учетом требований нормативных актов Банка России [6]—[8]; - бизнес- и технологических процессах, на непрерывность выполнения которых оказано влияние в результате реализации инцидента; - сроках и условиях, при которых будет восстановлено выполнение бизнес- и технологических процессов, в том числе восстановлено функционирование задействованных объектов информатизации; - предпринятых и запланированных действиях в рамках реагирования на инциденты и восстановления после их реализации, а также статусе выполнения соответствующих работ; - сведениях, которые могут быть раскрыты и доведены до потребителей финансовых услуг	О	О	О
ВРВ.44	Организация и выполнение деятельности по информированию причастных сторон (за исключением клиентов финансовой организации): - о влиянии реализации инцидента на непрерывность выполнения взаимосвязанных и взаимозависимых бизнес- и технологических процессов; - предпринятых и запланированных действиях в рамках реагирования на инциденты и восстановления после их реализации, а также статусе выполнения соответствующих работ	О	О	О
ВРВ.45	Организация и выполнение деятельности по информированию клиентов финансовой организации в рамках взаимодействия при реализации инцидентов: - о влиянии инцидента на предоставление финансовых и (или) информационных услуг, а также на конфиденциальность данных клиентов финансовой организации, в том числе их аутентификационных данных, используемых в рамках каналов дистанционного обслуживания; - планируемых сроках и условиях, которые необходимы для восстановления предоставления финансовой организацией финансовых и (или) информационных услуг;	О	О	О

Окончание таблицы 9

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВРВ.45	- рекомендуемых действиях, которые следует предпринять клиентам финансовой организации для снижения риска реализации информационных угроз	О	О	О
* Направление информации о фактах реализации инцидентов следует осуществлять в соответствии с установленными формами и сроками [35]. ** Финансовой организации должен быть определен порядок эскалации инцидентов [включая условия информирования совета директоров (наблюдательного совета), исполнительного органа финансовой организации], условия информирования причастных сторон, в том числе клиентов финансовой организации, а также сроки информирования об инцидентах, в том числе с учетом требований нормативных актов Банка России к информированию о событиях риска реализации информационных угроз, в частности [6]. Мера (в том числе меры ВРВ.42—ВРВ.45) применяется в отношении инцидентов, о которых следует информировать Банк России на основании требований нормативных актов Банка России [7], [8], [11]—[13], [33] в соответствии с установленными формами и сроками [35].				

7.5 Процесс 4 «Взаимодействие с поставщиками услуг»

7.5.1 Применяемые финансовой организацией меры по взаимодействию с поставщиками услуг 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.

Примечание — В рамках настоящего стандарта рассматривается часть деятельности по управлению риском, связанная с принятием мер, направленных на нейтрализацию информационных угроз (снижением СВР и ограничением СТП от реализации информационных угроз), обусловленных привлечением поставщиков услуг в сфере информационных технологий, в том числе защита объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг в сфере информационных технологий;

- управление риском технологической зависимости функционирования объектов информатизации финансовой организации от поставщиков услуг.

Примечание — В рамках настоящего стандарта рассматривается часть деятельности по управлению риском, связанная с принятием мер, направленных на нейтрализацию информационных угроз (снижением СВР и ограничением СТП от реализации информационных угроз), обусловленных технологической зависимостью функционирования объектов информационной инфраструктуры кредитной организации от поставщиков услуг в сфере информационных технологий.

При реализации процесса «Взаимодействие с поставщиками услуг» рекомендуется использовать ГОСТ Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, а также [36].

7.5.2 Состав мер по управлению риском реализации информационных угроз при привлечении поставщиков услуг, в том числе по защите объектов информатизации, входящих в критичную архитектуру, от возможной реализации информационных угроз, включая компьютерные атаки, со стороны поставщиков услуг применительно к уровням защиты приведен в таблице 10.

Таблица 10

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВПУ.1	Обнаружение и предотвращение вторжений (несанкционированных сетевых подключений) посредством объектов информатизации, используемых поставщиками услуг в рамках своей деятельности	Н	Т	Т
ВПУ.2	Разработка и применение процедур реагирования в случае реализации информационных угроз, в том числе компьютерных атак со стороны поставщиков услуг, а также в случае идентификации риска распространения вредоносного кода на вычислительные сети финансовой организации*	О	О	О

Окончание таблицы 10

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВПУ.3	Определение процедур по обеспечению безопасности цепи поставок (для целей обеспечения операционной надежности) в отношении поставщиков услуг, входящих в критичную архитектуру, включая:			
ВПУ.3.1	- определение приоритета в отношении поставщиков услуг, реализующих необходимые процедуры по обеспечению безопасности на этапах жизненного цикла поставляемых объектов информатизации, в том числе обеспечивающих «прозрачность» в отношении реализуемых ими процессов производства и сопровождения объектов информатизации, а также имеющих необходимую зрелость собственных процессов обеспечения безопасности цепи поставок, подтвержденную посредством проведения независимой оценки (внешнего аудита)**	Н	О	О
ВПУ.3.2	- анализ деятельности поставщиков услуг [в том числе до заключения соглашений на поставку объектов информатизации и (или) предоставление сторонних информационных сервисов], включая оценку реализуемых поставщиком услуг процедур по обеспечению безопасности на этапах жизненного цикла поставляемых объектов информатизации и минимизации риска их несанкционированной модификации на этапах поставки	Н	О	О
ВПУ.3.3	- оценку квалификации, опыта и репутации поставщиков услуг	О	О	О
ВПУ.3.4	- использование всевозможных источников информации для анализа и оценки поставщиков объектов информатизации и (или) сторонних информационных сервисов	О	О	О
ВПУ.3.5	- выявление слабостей или недостатков цепи поставок посредством проведения независимой оценки (внешнего аудита)**	Н	Н	О
ВПУ.3.6	- предварительную оценку (испытание, тестирование) объектов информатизации перед их использованием в качестве элементов критичной архитектуры (на этапах подбора или принятия в эксплуатацию, а также при их модернизации)	Н	Т	Т
ВПУ.4	Разработка и применение процедур по обеспечению безопасности цепи поставок в отношении процессов обеспечения операционной надежности финансовой организации, переданных на аутсорсинг, в том числе:			
ВПУ.4.1	- заключение соглашений об уровне оказания услуг (SLA) и неразглашении информации конфиденциального характера (NDA) в отношении поставщиков услуг***	О	О	О
ВПУ.4.2	- назначение основного и альтернативного поставщиков услуг (в том числе поставщика услуг, связанных с защитой от информационных угроз) в том случае, если основной поставщик услуг не сможет оказывать необходимый уровень услуг в кризисной ситуации*4	Н	О	О

* В частности, разработка и применение процедур изоляции и (или) блокирования сетевого взаимодействия с объектами информатизации поставщиков услуг, а также каналов взаимодействия, представляющих угрозу для вычислительных сетей и объектов информатизации финансовой организации.

** Принятие решений о проведении независимой оценки (внешнего аудита) следует осуществлять на основе риск-ориентированного подхода. Рекомендуется рассматривать проведение независимой оценки системы менеджмента безопасности цепи поставок согласно ГОСТ Р ИСО 28000.

*** Если для предоставления услуг финансовой организации поставщик заключает дополнительные договоры с подрядными организациями, в отношении данных подрядных организаций должны быть заключены SLA и NDA.

*4 Например, при реализации крупномасштабного инцидента.

7.5.3 Состав мер по управлению риском технологической зависимости функционирования объектов информатизации финансовой организации от поставщиков услуг применительно к уровням защиты приведен в таблице 11.

Таблица 11

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВПУ.5	Диверсификация риска нарушения поставок и сопровождения объектов информатизации, в том числе по государственной принадлежности*	Н	О	О
ВПУ.6	Включение в договор (контракт) о разработке объектов информатизации или поставке готовых объектов информатизации финансовым организациям положений по сопровождению (технической поддержке) и (или) техническому обслуживанию поставляемых изделий на планируемый срок их использования**	Н	О	О
ВПУ.7	Пролонгация договора (контракта) относительно сопровождения (технической поддержки) и (или) технического обслуживания поставляемых объектов информатизации, предусмотренного мерой ВПУ.6, в случае принятия решения о расширении ранее планируемого срока использования поставляемых объектов информатизации**	Н	О	О
ВПУ.8	Установление требований к обеспечению операционной надежности и защиты информации на этапах жизненного цикла проектируемых и разрабатываемых по заказу, а также приобретаемых объектов информатизации	О	О	О
ВПУ.9	Проведение на регулярной основе анализа эксплуатируемых финансовой организацией объектов информатизации с целью выявления продуктов, сопровождение (техническая поддержка и выпуск обновлений) которых поставщиками прекращено или планируется прекратить	О	О	О
ВПУ.10	Принятие решений по объектам информатизации, сопровождение (техническая поддержка и выпуск обновлений) которых поставщиками прекращено, включая: - отказ от эксплуатации и замену объектов информатизации, сопровождение (техническая поддержка и выпуск обновлений) которых поставщиками прекращено; - обоснование и документирование (фиксация) решения о дальнейшей эксплуатации объектов информатизации (их компонентов), сопровождение (техническая поддержка и выпуск обновлений) которых поставщиками прекращено	О	О	О
ВПУ.11	Организация сопровождения (технической поддержки и выпуска обновлений) объектов информатизации, сопровождение которых поставщиками прекращено, самостоятельно или посредством привлечения альтернативных поставщиков, включая разработку, применение и контроль дополнительных мер, направленных на устранение уязвимостей таких объектов информатизации***	О	О	О
ВПУ.12	Своевременное, планируемое и контролируемое техническое обслуживание объектов информатизации прикладного и инфраструктурного уровней, входящих в критичную архитектуру, в том числе:			
ВПУ.12.1	- авторизация и регистрация операций, осуществляемых в рамках технического обслуживания, а также аутентификация осуществляющих их субъектов доступа	Н	Т	Т

Продолжение таблицы 11

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ВПУ.12.2	- контроль соблюдения требований к обеспечению защиты информации в процессе технического обслуживания, направленных на обеспечение целостности, конфиденциальности и доступности информации	О	О	О
ВПУ.12.3	- проведение технического обслуживания в соответствии со спецификациями (техническими требованиями и условиями) поставщиков объектов информатизации и (или) требованиями финансовой организации	О	О	О
ВПУ.12.4	- тестирование (проверка) работоспособности объектов информатизации после проведения технического обслуживания для выявления риска нарушения операционной надежности	Н	Т	Т
ВПУ.13	Контроль удаленного технического обслуживания и диагностики, осуществляемых при подключении извне вычислительных сетей финансовой организации, в том числе предусматривающий:			
ВПУ.13.1	- многофакторную аутентификацию субъектов доступа, осуществляющих удаленное техническое обслуживание и диагностику	О	Т	Т
ВПУ.13.2	- регистрацию операций, осуществляемых в рамках удаленного технического обслуживания и диагностики объектов информатизации;	Т	Т	Т
ВПУ.13.3	- завершение сессии и прерывание сетевого подключения субъектов доступа после окончания удаленного технического обслуживания	Н	О	Т
ВПУ.13.4	- последующий контроль и анализ операций, осуществляемых в рамках удаленного технического обслуживания и диагностики	О	О	О
ВПУ.13.5	- установление в договорах (контрактах) требований к осуществлению удаленного технического обслуживания и диагностики только посредством объектов информатизации, в отношении которых реализован тот же уровень защиты (в том числе защиты информации), который применяется для обслуживаемых объектов информатизации	Т	Т	Т
ВПУ.13.6	- использование защищенного выделенного (виртуального) канала сетевого взаимодействия при удаленном техническом обслуживании	Т	Т	Т
ВПУ.13.7	- применение средств защиты информации для защиты целостности и конфиденциальности сессий сетевого взаимодействия при удаленном техническом обслуживании и диагностике	Т	Т	Т
ВПУ.13.8	- контроль и подтверждение завершения сессий и прерывания сетевого подключения субъектов доступа после окончания удаленного технического обслуживания и диагностики	Н	Т	Т
ВПУ.14	Привлечение к сопровождению и техническому обслуживанию объектов информатизации финансовой организации лиц, обладающих соответствующей квалификацией	О	О	О
[*] Для диверсификации риска нарушения поставок и сопровождения объектов информатизации по государственной принадлежности финансовые организации в том числе могут применять следующие меры: - планирование и реализация мероприятий по замещению импортозависимого программного и аппаратного обеспечения; - тестирование возможности использования программного и аппаратного обеспечения, произведенного компаниями, не подверженными санкционным рискам;				

Окончание таблицы 11

- тестирование возможности использования ПО с открытым исходным кодом, применение которого не ограничивается каким-либо юридическим лицом;
- планирование, на случай возникновения такой необходимости, мероприятий по переходу к использованию программного и аппаратного обеспечения, произведенного компаниями, не подверженными санкционным рискам, и (или) ПО с открытым исходным кодом, использование которого не ограничивается каким-либо юридическим лицом;
- приобретение достаточного запаса аппаратного обеспечения и комплектующих к нему для осуществления оперативного ремонта без привлечения поставщиков продуктов и/или контрагентов, а также для обеспечения необходимого резерва вычислительных мощностей и дискового пространства на время переходного периода;
- закупка ПО иностранного производства путем приобретения неисключительных прав на использование в собственность финансовых организаций вместо срочной подписки, а также безлимитных лицензий;
- привлечение поставщиков услуг (в том числе поставщиков облачных услуг), в том числе приобретение услуг поддержки ПО, серверного и телекоммуникационного оборудования у компаний, деятельность которых менее подвержена влиянию санкционных рисков.

** В случае невозможности включения в договор (контракт) указанных положений должен быть приобретен полный комплект документации, обеспечивающий возможность сопровождения объектов информатизации без участия разработчика.

Комплект документации в том числе должен включать:
- документацию администрирования, содержащую инструкции и (или) рекомендации по безопасному конфигурированию, установке и эксплуатации объектов информатизации;
- документацию администрирования, содержащую инструкции и (или) рекомендации по применению настроек или мер безопасности;
- пользовательскую документацию, содержащую сведения о доступных мерах безопасности, а также инструкции и (или) рекомендации по их применению;
- пользовательскую документацию, содержащую инструкции и (или) рекомендации по безопасной работе пользователя с объектами информатизации.

Если оба указанных варианта неприемлемы, например вследствие высокой стоимости или позиции поставщика (разработчика), лица, принимающие решения на стороне финансовой организации, должны оценить и зафиксировать допустимость риска реализации информационных угроз, возникающего при невозможности сопровождения объектов информатизации.

*** В случае отсутствия возможности отказа от эксплуатации таких объектов информатизации.

7.6 Процесс 5 «Тестирование операционной надежности бизнес- и технологических процессов»

7.6.1 Применяемые финансовой организацией меры по тестированию операционной надежности бизнес- и технологических процессов должны обеспечивать 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).

При реализации процесса «Тестирование операционной надежности бизнес- и технологических процессов» также рекомендуется использовать [37].

7.6.2 Состав мер по проведению сценарного анализа и тестирования с использованием его результатов готовности финансовой организации противостоять реализации информационных угроз в отношении критичной архитектуры (киберучения) применительно к уровням защиты приведен в таблице 12.

Таблица 12

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ТОН.1	Установление и реализация программ по сценарному анализу и тестированию готовности финансовой организации противостоять реализации информационных угроз, включая:			
ТОН.1.1	- формирование сценариев реализации информационных угроз, в том числе компьютерных атак	Н	О	О

Продолжение таблицы 12

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ТОН.1.2	- тестирование возможностей по мониторингу и выявлению фактов реализации информационных угроз	О	О	О
ТОН.1.3	- тестирование процедур реагирования на инциденты и восстановления после их реализации	О	О	О
ТОН.1.4	- тестирование сценариев, предусматривающих сдерживание и (или) предотвращение реализации компьютерных атак и их последовательностей, в том числе на разных уровнях информационной инфраструктуры с учетом технического описания таких сценариев	Н	О	О
ТОН.1.5	- оценку подготовленности работников финансовой организации противостоять реализации информационных угроз, в том числе компьютерных атак	О	О	О
ТОН.1.6	- оценку достаточности ресурсного (кадрового и материального) обеспечения для реагирования на инциденты и восстановления после их реализации	О	О	О
ТОН.2	Определение во внутренних документах финансовой организации методологии (за исключением случаев привлечения поставщиков услуг) и порядка проведения сценарного анализа и тестирования готовности финансовой организации противостоять реализации информационных угроз	О	О	О
ТОН.3	Организация и выполнение деятельности по формированию и регулярному пересмотру сценариев реализации информационных угроз на основе информации: - об инцидентах, характерных для вида деятельности финансовой организации*; - инцидентах, характерных для технологических участков бизнес- и технологических процессов; - проведенных ранее тестированиях готовности финансовой организации противостоять реализации информационных угроз; - актуальных сценариях реализации информационных угроз, в том числе компьютерных атак	О	О	О
ТОН.4	Организация и выполнение деятельности по тестированию готовности финансовой организации противостоять реализации информационных угроз на основе сформированных сценариев, включая: - выявление конфигураций объектов информатизации, имеющих слабости и (или) уязвимости; - выявление актуальных слабостей (уязвимостей) используемых объектов информатизации; - определение актуальных компьютерных атак, которые могут быть реализованы путем эксплуатации выявленных уязвимостей; - определение вероятных инцидентов, связанных с реализацией информационных угроз, к которым может привести реализация актуальных компьютерных атак; - определение потенциальных последствий от реализации инцидентов, в том числе максимально возможных финансовых потерь	Н	О	О
ТОН.5	Организация и выполнение деятельности по тестированию возможностей мониторинга и выявления на предмет своевременного обнаружения фактов реализации информационных угроз (в том числе компьютерных атак), а также контроль актуальности используемых данных об индикаторах компрометации объектов информатизации	Н	О	Т

Продолжение таблицы 12

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ТОН.6	Организация и выполнение деятельности по тестированию процедур реагирования на инциденты и восстановления после их реализации, в том числе совместно с причастными сторонами в целях:			
ТОН.6.1	- тестирования возможности финансовой организации обеспечить эффективное реагирование на инциденты и восстановление после их реализации в соответствии с заданными временными периодами (ЦВВ)	О	О	О
ТОН.6.2	- тестирования возможности финансовой организации совместно с причастными сторонами обеспечить эффективное реагирование на инциденты и восстановление после их реализации в соответствии с заданными временными периодами (ЦВВ), в том числе в отношении переданных на аутсорсинг бизнес- и технологических процессов	О	О	О
ТОН.6.3	- тестирования возможностей финансовой организации обеспечить эффективное взаимодействие с причастными сторонами при реализации инцидентов	О	О	О
ТОН.6.4	- тестирования возможности финансовой организации обеспечить своевременное информирование об инцидентах Банка России, федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также причастных сторон	О	О	О
ТОН.7	Установление точных целей в рамках каждого из проводимых тестирований готовности финансовой организации противостоять реализации информационных угроз и целевых показателей, посредством которых оценивают их достижение	О	О	О
ТОН.8	Разработка и использование в рамках тестирования готовности финансовой организации противостоять реализации информационных угроз, в том числе сценариев, реализующих методы: - «социальной инженерии» [побуждения работников финансовой организации к осуществлению операций (действий) путем обмана или злоупотребления доверием]; - «фишинга» (использование информации, вводящей работников финансовых организаций в заблуждение относительно принадлежности информации, распространяемой посредством сети Интернет, вследствие сходства доменных имен, оформления или содержания)	О	О	О
ТОН.9	Разработка и использование сценариев, предполагающих значительное влияние на деятельность финансовой организации (включая существенные финансовые потери)**, для определения потенциала такого влияния и оценки риска реализации информационных угроз (стресс-тестирование***), предусмотренной в рамках ГОСТ Р 57580.3	Н	Н	О
ТОН.10	Информирование коллегиального исполнительного органа и должностного лица, ответственного за функционирование системы управления риском реализации информационных угроз, о результатах проведения стресс-тестирования, предусмотренного мерой ТОН.9	Н	Н	О
ТОН.11	Определение и анализ показателей оценки эффективности программ тестирования готовности финансовой организации противостоять реализации информационных угроз	О	О	О
ТОН.12	Использование результатов мониторинга и анализа показателей оценки эффективности программ тестирования готовности финансовой организации противостоять реализации информационных угроз для последующей доработки (совершенствования) таких программ	О	О	О

Окончание таблицы 12

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ТОН.13	Разработка сценариев и проведение периодических тестирований готовности финансовой организации противостоять реализации информационных угроз в условиях, приближенных к реальным, с привлечением: - структурных подразделений финансовой организации и должностных лиц, принимающих решения в рамках реагирования на инциденты и восстановления после их реализации; - ключевых причастных сторон (за исключением клиентов финансовой организации)	Н	Н	О
ТОН.14	Участие финансовой организации (при наличии возможности) в тестированиях готовности противостоять реализации информационных угроз, проводимых иными организациями, в том числе в рамках соответствующих мероприятий межсекторального и трансграничного характера	Н	Н	Н

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

** Рекомендуется в рамках тестирования таких сценариев предусмотреть возможность привлечения коллегиального исполнительного органа, единоличного исполнительного органа и (или) подотчетных им коллегиальных органов.

*** Результаты стресс-тестирований должны быть учтены в рамках совершенствования системы управления риском реализации информационных угроз финансовой организации, предусмотренной в рамках ГОСТ Р 57580.3.

7.7 Процесс 6 «Защита критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы»

7.7.1 Финансовая организация должна применять меры по защите критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы.

7.7.2 Состав мер по защите критичной архитектуры от возможной реализации информационных угроз в условиях удаленной работы применительно к уровням защиты приведен в таблице 13.

Таблица 13

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ЗУР.1	Разработка отдельного плана или соответствующих положений в рамках плана ОНиВД* по переводу, в случае необходимости, работников финансовой организации (значительной части сотрудников) на дистанционный формат работы вне основных офисов финансовой организации, в частности из дома («удаленная работа»), в том числе на длительный срок	О	О	О
ЗУР.2	Планирование и управление пропускной способностью средств защиты информации, реализующих защищенный удаленный логический доступ при переводе работников финансовой организации (значительной части сотрудников) на дистанционный формат работы вне основных офисов финансовой организации, в частности из дома («удаленная работа»)	О	О	О
ЗУР.3	Обеспечение и контроль соблюдения требований и выполнения мер, направленных на реализацию процесса «Защита информации при осуществлении удаленного логического доступа с использованием мобильных (переносных) устройств», предусмотренных ГОСТ Р 57580.1	О	О	О

* План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности финансовой организации в случае возникновения прерываний.

7.8 Процесс 7 «Управление риском внутреннего нарушителя»

7.8.1 Финансовая организация должна применять меры по управлению риском внутреннего нарушителя.

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

7.8.2 Состав мер по управлению риском внутреннего нарушителя применительно к уровням защиты приведен в таблице 14.

Таблица 14

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
РВН.1	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска внутреннего нарушителя, применяемых в отношении работников финансовой организации, деятельность которых может оказать влияние на риск реализации информационных угроз: - при приеме на работу кандидатов на замещение должностей в финансовой организации; - в рамках исполнения работниками своих должностных обязанностей; - в случае прекращения трудовых отношений или изменения должностных обязанностей работников	О	О	О
РВН.2	Включение в состав мероприятий, предусмотренных мерой РВН.1, при приеме на работу кандидатов на замещение должностей, деятельность которых может оказать влияние на риск реализации информационных угроз:			
РВН.2.1	- оценки профессиональных навыков и соответствия кандидата квалификационным требованиям, предъявляемым финансовой организацией	О	О	О
РВН.2.2	- выявление факторов, являющихся побудительными или стимулирующими к использованию кандидатом предоставленных полномочий для реализации информационных угроз	Н	О	О
РВН.2.3	- проверку подлинности предоставленных кандидатом документов, заявленного уровня квалификации, точности и полноты предоставленных данных	О	О	О
РВН.2.4	- рассмотрение рекомендаций предыдущих работодателей, в случае необходимости	Н	О	О
РВН.3	Включение в состав мероприятий, предусмотренных мерой РВН.1, в рамках исполнения работниками своих должностных обязанностей, деятельность которых может оказать влияние на риск реализации информационных угроз:			
РВН.3.1	- включение в трудовые контракты (соглашения, договоры) и (или) должностные инструкции и доведение до работников финансовой организации обязанностей по соблюдению соответствующих требований, а также ответственности за их нарушение	О	О	О
РВН.3.2	- проведение проверок на регулярной основе с учетом полномочий работников по доступу к объектам информатизации, задействованным при выполнении бизнес- и технологических процессов	Н	О	О
РВН.3.3	- проведение внеплановых проверок при выявлении фактов причастности работников к реализации инцидентов	Н	О	О

Продолжение таблицы 14

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
РВН.3.4	- приравнивание фактов невыполнения работниками финансовой организации требований к обеспечению операционной надежности и защиты информации к фактам неисполнения должностных обязанностей и применение в указанных случаях соответствующих дисциплинарных взысканий согласно Трудовому кодексу Российской Федерации	О	О	О
РВН.3.5	- регистрация фактов применения дисциплинарных взысканий согласно Трудовому кодексу Российской Федерации в отношении работников, нарушивших требования к обеспечению операционной надежности и защите информации, с указанием причин применения таких взысканий	О	О	О
РВН.4	Включение в состав мероприятий, предусмотренных мерой РВН.1, в случае прекращения трудовых отношений или изменения должностных обязанностей работников, деятельность которых может оказать влияние на риск реализации информационных угроз:			
РВН.4.1	- применение соответствующих мер в рамках процесса управления учетными записями и правами субъектов логического доступа, требования к которому определены в ГОСТ Р 57580.1	О	О	О
РВН.4.2	- пересмотр потребности работника в доступе к отдельным объектам информатизации	Н	О	О
РВН.4.3	- организация и контроль возврата всех принадлежащих финансовой организации объектов информатизации, переданных соответствующему работнику в рамках исполнения им должностных обязанностей	О	О	О
РВН.4.4	- обеспечение возможности в течение определенного временного периода доступа к защищаемой информации*, использовавшейся работниками финансовой организации до прекращения с ними трудовых отношений или изменения должностных обязанностей	Н	О	Т
РВН.5	Планирование, реализация, контроль и совершенствование мероприятий, направленных на уменьшение негативного влияния риска внутреннего нарушителя, применяемых в отношении работников поставщика услуг, привлекаемого в рамках выполнения бизнес- и технологических процессов	О	О	О
РВН.6	Включение в состав мероприятий, предусмотренных мерой РВН.5:			
РВН.6.1	- установление в рамках договорных отношений требований к соблюдению работниками поставщиков услуг установленных финансовой организацией требований к обеспечению операционной надежности и защите информации, а также их обязанностей и ответственности	О	О	О
РВН.6.2	- установление в рамках договорных отношений требований к поставщикам услуг по уведомлению о случаях изменения должностных обязанностей или прекращения трудовых отношений с работниками, обладающими организационными полномочиями или привилегированным доступом к объектам информатизации финансовой организации	О	О	О
РВН.6.3	- осуществление контроля за выполнением поставщиком требований, установленных в рамках договорных отношений	О	О	О
РВН.7	Реализация программ по мотивации работников финансовой организации к соблюдению установленных требований к обеспечению операционной надежности и защиты информации:			
РВН.7.1	- разработка и применение способов мотивации работников к участию в процессах управления риском реализации информационных угроз	Н	О	О

Окончание таблицы 14

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
РВН.7.2	- разработка и применение способов мотивации персонала к направлению предложений по мероприятиям, направленным на уменьшение негативного влияния риска реализации информационных угроз	Н	О	О
РВН.7.3	- разработка справочных материалов и инструкций для работников по вопросам противостояния реализации информационных угроз	Н	О	О
РВН.7.4	- разработка и применение способов мотивации работников к инициативному информированию о возможном риске реализации информационных угроз и о выявленных событиях реализации информационных угроз	Н	О	О
* К защищаемой информации относится информация, перечень которой определен в [11]—[13].				

7.9 Процесс 8 «Обеспечение осведомленности об актуальных информационных угрозах»

7.9.1 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.

7.9.2 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 таблице 15.

Таблица 15

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.1	Организация и выполнение деятельности по получению от причастных сторон (за исключением клиентов финансовой организации) и по направлению информации о возможных сценариях реализации информационных угроз*	О	О	О
ОСО.2	Организация и выполнение деятельности по получению от Банка России и по направлению информации о возможных сценариях реализации информационных угроз с использованием технической инфраструктуры Банка России*	О	О	О
ОСО.3	Организация и выполнение деятельности по получению информации о возможных сценариях реализации информационных угроз от доверенных внешних организаций, в том числе в рамках участия в соответствующих сообществах	Н	О	О
ОСО.4	Включение в состав передаваемой информации о возможных сценариях реализации информационных угроз результатов анализа причин и последствий реализации инцидентов**, предусмотренного в рамках процесса 3 «Выявление, регистрация, реагирование на инциденты, связанные с реализацией информационных угроз, и восстановление после их реализации»	Н	О	О

Окончание таблицы 15

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.5	Организация и выполнение деятельности по доведению до клиентов финансовой организации информации, способствующей повышению их готовности противостоять реализации информационных угроз и снижению негативного влияния риска реализации информационных угроз при предоставлении (получении) финансовых и (или) информационных услуг, включая справочные материалы в части: - корректного использования ПО (в том числе электронных средств платежа), используемого в целях осуществления финансовых (банковских) операций, включая операции по переводу денежных средств; - правильного обращения с информацией конфиденциального характера; - возможных сценариев реализации информационных угроз (в частности, компьютерных атак, реализуемых посредством применения вредоносного ПО, фишинга и методов социальной инженерии), направленных на клиентов финансовой организации, и способов их выявления	О	О	О
ОСО.6	Организация и выполнение деятельности по обеспечению максимальной доступности для клиентов финансовой организации справочных материалов, предусмотренных мерой ОСО.5	О	О	О
ОСО.7	Организация и выполнение деятельности по оценке эффективности реализуемых программ по доведению до клиентов финансовой организации информации, способствующей повышению их готовности противостоять реализации информационных угроз и уменьшению негативного влияния риска реализации информационных угроз при предоставлении (получении) финансовых и (или) информационных услуг	О	О	О
ОСО.8	Организация и выполнение деятельности по доведению до клиентов финансовой организации (с обеспечением максимальной доступности) фактических значений КПУР, приведенных в строках 3—8 таблицы Д.2 приложения Д ГОСТ Р 57580.3—2022	О	О	О

* При наличии соответствующих договорных обязательств.

При наличии возможности финансовым организациям также рекомендуется обмениваться позитивным опытом применения мер обеспечения операционной надежности в части выявления, регистрации, реагирования на инциденты и восстановления функционирования бизнес- и технологических процессов и объектов информатизации после их реализации.

** В рамках обмена информацией о возможных сценариях реализации информационных угроз с причастными сторонами финансовая организация самостоятельно определяет возможность раскрытия, а также объем и формат раскрываемой информации.

7.9.3 Состав мер по использованию информации об актуальных сценариях реализации информационных угроз для цели обеспечения операционной надежности финансовой организации применительно к уровням защиты приведен в таблице 16.

Таблица 16

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.9	Организация и выполнение деятельности по оценке возможности применения информации об актуальных сценариях реализации информационных угроз, получение которой предусмотрено мерами ОСО.1—ОСО.3 в таблице 15	О	О	О

Окончание таблицы 16

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.10	Организация и выполнение деятельности по использованию информации об актуальных сценариях реализации информационных угроз, получение которой предусмотрено мерами ОСО.1—ОСО.3 в таблице 15, для цели обеспечения операционной надежности финансовой организации	О	Т	Т

7.9.4 Состав мер по повышению осведомленности работников финансовой организации в части противостояния реализации информационных угроз применительно к уровням защиты приведен в таблице 17.

Таблица 17

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.11	Повышение осведомленности по вопросам противостояния реализации информационных угроз членов совета директоров (наблюдательного совета) и исполнительного органа финансовой организации, в том числе по вопросам организации и контроля за управлением риском реализации информационных угроз, за обеспечением операционной надежности и защиты информации*	О	О	О
ОСО.12	Организация и контроль со стороны исполнительного органа финансовой организации деятельности по обучению и повышению осведомленности работников финансовой организации в части противостояния реализации информационных угроз, включая разработку и реализацию соответствующих планов по периодическому обучению и повышению осведомленности работников финансовой организации	Н	О	О
ОСО.13	Включение в разрабатываемые для различных групп работников (с учетом их должностных обязанностей и выполняемых ролей) планы обучения и повышения осведомленности в части противостояния реализации информационных угроз учебных мероприятий по доведению: - информации, содержащейся в утвержденной политике управления риском реализации информационных угроз финансовой организации; - информации о применяемых в финансовой организации мерах, направленных на управление риском реализации информационных угроз, на обеспечение операционной надежности и защиты информации; - информации о возможных сценариях реализации компьютерных атак, направленных на работников финансовой организации (в частности, компьютерных атак, реализуемых посредством применения вредоносного ПО, фишинга и методов социальной инженерии); - инструкций по выполнению мер, направленных на противостояние реализации информационных угроз, в соответствии с внутренними документами финансовой организации; - информации о значимости и важности деятельности работников финансовой организации в рамках управления риском реализации информационных угроз, обеспечения операционной надежности и защиты информации; - инструкций по порядку и способам взаимодействия при реализации инцидентов, связанных с реализацией информационных угроз	Н	О	О
ОСО.14	Организация обучения или инструктажа** работника, получившего новую роль, с последующим проведением оценочных мероприятий по вопросам противостояния реализации информационных угроз и доведением результатов указанных мероприятий до работника, принимавшего в них участие	О	О	О

Окончание таблицы 17

Условное обозначение и номер меры	Содержание мер системы обеспечения операционной надежности	Уровень защиты		
		3	2	1
ОСО.15	Организация обучения или инструктажа в части выявления и инициативного информирования о событиях риска реализации информационных угроз	О	О	О

* В отношении мероприятий по повышению осведомленности совета директоров (наблюдательного совета) и исполнительного органа финансовая организация самостоятельно определяет условия их проведения, например:

- на регулярной основе;
- при возникновении определенных условий, свидетельствующих о необходимости проведения таких мероприятий;
- по запросу со стороны участника или участников целевой группы таких мероприятий.

** Согласно разработанным для различных групп работников (с учетом их должностных обязанностей и выполняемых ролей) программам обучения и повышения осведомленности в части выявления и противостояния реализации информационных угроз.

8 Требования к системе организации и управления операционной надежностью финансовой организации

8.1 Общие положения

8.1.1 Настоящий раздел устанавливает требования к содержанию базового состава мер обеспечения операционной надежности, входящих в состав системы организации и управления операционной надежностью, направленных на обеспечение должной полноты и качества реализации системы обеспечения операционной надежности.

8.1.2 Меры системы организации и управления операционной надежностью применяют для каждого отдельного процесса обеспечения операционной надежности из числа определенных в разделе 7.

8.1.3 Меры системы организации и управления операционной надежностью применяют в рамках следующих направлений:

- направление 1 «Планирование процесса системы обеспечения операционной надежности» («Планирование»);
- направление 2 «Реализация процесса системы обеспечения операционной надежности» («Реализация»);
- направление 3 «Контроль процесса системы обеспечения операционной надежности» («Контроль»);
- направление 4 «Совершенствование процесса системы обеспечения операционной надежности» («Совершенствование»).

8.1.4 Способы реализации мер системы организации и управления операционной надежностью, установленные в таблицах 18—21, обозначены так же, как и в 7.1.2.

8.2 Направление 1 «Планирование процесса системы обеспечения операционной надежности»

8.2.1 В рамках направления «Планирование» финансовая организация обеспечивает определение (пересмотр):

- области применения процесса обеспечения операционной надежности;
- состава применяемых (а также неприменяемых) мер обеспечения операционной надежности из числа мер, определенных в разделах 7 и 8;
- состава и содержания мер обеспечения операционной надежности, являющихся дополнительными к базовому составу мер, приведенных в разделах 7 и 8, определяемых на основе актуальных информационных угроз;
- порядка применения мер обеспечения операционной надежности в рамках процесса обеспечения операционной надежности.

Деятельность в рамках направления «Планирование» реализуется согласно политике финансовой организации в отношении принятого допустимого уровня риска реализации информационных угроз, сигнальных и контрольных значений КПУР, предусмотренных ГОСТ Р 57580.3, а также допустимого уровня простоя и (или) деградации бизнес- и технологических процессов. При необходимости реализация деятельности в рамках направления «Планирование» осуществляется на основе результатов деятельности в рамках направления «Совершенствование».

8.2.2 Базовый состав мер планирования процесса системы обеспечения операционной надежности приведен в таблице 18.

Таблица 18

Условное обозначение и номер меры	Содержание мер системы организации и управления операционной надежностью	Уровень защиты		
		3	2	1
ПОН.1	Документарное определение области применения процесса системы обеспечения операционной надежности в отношении идентифицированных элементов критичной архитектуры	О	О	О
ПОН.2	Определение подходов к идентификации и включению элементов критичной архитектуры в область применения процесса обеспечения операционной надежности	О	О	О
ПОН.3	Документарное определение состава (с указанием соответствия настоящему стандарту) и содержания организационных и технических мер обеспечения операционной надежности, выбранных финансовой организацией и реализуемых в рамках процесса обеспечения операционной надежности	О	О	О
ПОН.4	Документарное определение порядка применения организационных и технических мер обеспечения операционной надежности (процедур в рамках процесса обеспечения операционной надежности), реализуемых в рамках процесса системы обеспечения операционной надежности	О	О	О
ПОН.5	Определение ролей, полномочий и ответственности должностных лиц, задействованных при реализации процесса операционной надежности	О	О	О
ПОН.6	Определение порядка принятия решений при реализации процесса обеспечения операционной надежности, интеграция порядка принятия решений (или делегирования прав принятия решений) в структуру корпоративного управления финансовой организации	О	О	О
ПОН.7	Определение состава, подходов и требований к организации ресурсного обеспечения процесса обеспечения операционной надежности, в том числе технологического, технического и кадрового обеспечения*	О	О	О
ПОН.8	Распределение ответственности в рамках реализации процесса обеспечения операционной надежности при привлечении поставщиков услуг (в том числе поставщиков облачных услуг)	О	О	О

* Рекомендуется использовать [37].

8.3 Направление 2 «Реализация процесса системы обеспечения операционной надежности»

8.3.1 Деятельность в рамках направления «Реализация» осуществляется по результатам выполнения направлений «Планирование» и (или) «Совершенствование» (см. 8.2 и 8.5 соответственно).

В рамках направления «Реализация» финансовая организация обеспечивает:

- 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.

8.3.2 Базовый состав мер по реализации процесса системы обеспечения операционной надежности приведен в таблице 19.

Таблица 19

Условное обозначение и номер меры	Содержание мер системы организации и управления операционной надежностью	Уровень защиты		
		3	2	1
РОН.1	Реализация эксплуатации (в том числе использования по назначению) технических мер обеспечения операционной надежности	О	О	О
РОН.2	Реализация применения организационных мер обеспечения операционной надежности	О	О	О
РОН.3	Назначение ответственных лиц за выполнение ролей по обеспечению операционной надежности с учетом необходимости обеспечения снижения риска возникновения конфликта интересов*	О	О	О
РОН.4	Обеспечение доступности технических мер обеспечения операционной надежности: - применение отказоустойчивых технических решений; - резервирование аппаратных, программных, аппаратно-программных средств и (или) систем, необходимых для функционирования технических мер обеспечения операционной надежности; - осуществление контроля безотказного функционирования аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности; - принятие регламентированных мер по восстановлению отказавших аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности	Н	Н	Т
РОН.5	Обеспечение возможности сопровождения аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности в течение всего срока их использования	Н	О	О
РОН.6	Обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер обеспечения операционной надежности в рамках процесса обеспечения операционной надежности	О	О	О
РОН.7	Повышение осведомленности (инструктаж) работников финансовой организации в области реализации процесса обеспечения операционной надежности, применения организационных мер обеспечения операционной надежности, использования по назначению аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности	О	О	О

* В частности:

- назначение работников финансовой организации, ответственных за реализацию контрольных процедур в рамках процесса управления изменениями в части управления конфигурациями объектов информатизации, из числа работников финансовой организации, которые не вовлечены в разработку объектов информатизации;
- разделение (где это возможно) ролей, связанных с реализацией процессов обеспечения операционной надежности и с контролем за их реализацией.

8.4 Направление 3 «Контроль процесса системы обеспечения операционной надежности»

8.4.1 Деятельность в рамках направления «Контроль» должна гарантировать принятие мер обеспечения операционной надежности, осуществляемых надлежащим образом и соответствующих политике финансовой организации в отношении принятого допустимого уровня риска реализации информационных угроз (риск аппетита).

Применяемые финансовой организацией меры должны обеспечивать контроль:

- области применения процесса обеспечения операционной надежности;
- должного применения организационных и технических мер;
- знаний работников финансовой организации в части принятия организационных и технических мер.

8.4.2 Базовый состав мер контроля процесса системы обеспечения операционной надежности приведен в таблице 20.

Таблица 20

Условное обозначение и номер меры	Содержание мер системы организации и управления операционной надежностью	Уровень защиты		
		3	2	1
КОН.1	Контроль применения процесса обеспечения операционной надежности в отношении фактического состава идентифицированных элементов критичной архитектуры, входящих в область применения процесса обеспечения операционной надежности	О	О	О
КОН.2	Контроль эксплуатации (в том числе использования по назначению) аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности, включая: - контроль назначения ролей, связанных с эксплуатацией аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности; - контроль выполнения руководства и (или) порядка по эксплуатации аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности	О	О	О
КОН.3	Периодический контроль (тестирование) полноты реализации технических мер обеспечения операционной надежности	О	Т	Т
КОН.4	Контроль применения организационных мер обеспечения операционной надежности	О	О	О
КОН.5	Контроль безотказного функционирования аппаратных, программных, аппаратно-программных средств и (или) систем, реализующих технические меры обеспечения операционной надежности, а также обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и систем, а также их тестирование (проверка)	О	Т	Т
КОН.6	Проведение проверок знаний работников финансовой организации в части применения мер обеспечения операционной надежности	О	О	О
КОН.7	Фиксация результатов (свидетельств) проведения мероприятий по контролю реализации процесса обеспечения операционной надежности	О	О	О

8.5 Направление 4 «Совершенствование процесса системы обеспечения операционной надежности»

8.5.1 Деятельность в рамках направления «Совершенствование» выполняется на основе результатов проведения мероприятий по выявлению, реагированию на инциденты и по восстановлению после их реализации, по обнаружению недостатков в обеспечении операционной надежности в рамках направления «Контроль», а также в случаях изменения политики финансовой организации в отношении принципов и приоритетов в реализации системы обеспечения операционной надежности, принятого допустимого уровня риска реализации информационных угроз (риск-аппетита), сигнальных и контрольных значений КПУР, а также допустимого уровня простоя и (или) деградации бизнес- и технологических процессов, предусмотренных ГОСТ Р 57580.3.

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. При этом непосредственная деятельность по совершенствованию процесса обеспечения операционной надежности осуществляется в рамках направления «Реализация» и, при необходимости, направления «Планирование».

8.5.2 Базовый состав мер по совершенствованию процесса системы обеспечения операционной надежности приведен в таблице 21.

Таблица 21

Условное обозначение и номер меры	Меры обеспечения операционной надежности	Уровень защиты		
		3	2	1
СОН.1	Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы обеспечения операционной надежности в случаях обнаружения: - инцидентов, связанных с реализацией информационных угроз (отнесенных финансовой организацией к событиям риска реализации информационных угроз, приведенных в ГОСТ 57580.3); - недостатков в рамках контроля системы обеспечения операционной надежности	О	О	О
СОН.2	Проведение и фиксация результатов (свидетельств) анализа необходимости совершенствования процесса системы обеспечения операционной надежности в случаях изменения политики финансовой организации в отношении: - области применения процесса обеспечения операционной надежности; - основных принципов и приоритетов в реализации процесса системы обеспечения операционной надежности; - принятого допустимого уровня риска реализации информационных угроз (риск-аппетита)*, сигнальных и контрольных значений КПУР (а также целевых показателей операционной надежности), предусмотренных ГОСТ Р 57580.3 и приложением Б с учетом требований нормативных актов Банка России [6]—[8]	О	О	О
СОН.3	Фиксация решений о проведении совершенствования процесса системы обеспечения операционной надежности в виде корректирующих или превентивных действий, например: - пересмотр области применения процесса системы обеспечения операционной надежности; - пересмотр состава и содержания организационных мер обеспечения операционной надежности, применяемых в рамках процесса системы обеспечения операционной надежности; - пересмотр состава технических мер обеспечения операционной надежности, применяемых в рамках процесса системы обеспечения операционной надежности	О	О	О
СОН.4	Организация и выполнение деятельности по совершенствованию** применяемых организационных и технических мер, в том числе на основе информации, полученной: - по результатам анализа причин и последствий реализации инцидентов; - в рамках консультаций с экспертами внутри финансовой организации***	О	О	О

* Агрегированный показатель, учитывающий принятые финансовой организацией контрольные значения КПУР и значимость группы КПУР в зависимости от вида деятельности финансовой организации.

** В рамках совершенствования применяемых организационных и технических мер обеспечения операционной надежности рекомендуется проводить мониторинг и анализ внешних информационных ресурсов для своевременной адаптации к изменяющимся внешним условиям, обусловленным:

- изменением ландшафта информационных угроз;
- изменением в нормативном регулировании соответствующей сферы;
- появлением новейших технологических решений, а также публикациями лучших практик в данной области.

*** При наличии возможности для консультаций могут быть привлечены внешние эксперты.

Приложение А
(справочное)

Перечень технологических мер защиты информации

А.1 Перечень технологических мер защиты информации, определяемый согласно требованиям нормативных актов Банка России [11]—[13], обрабатываемой в рамках технологических операций (участков) бизнес- и технологических процессов, приведен в таблице А.1.

Таблица А.1

Технологические операции (участки) бизнес- и технологических процессов	Технологические меры
Идентификация, аутентификация и авторизация клиентов финансовой организации в целях осуществления финансовых (банковских) операций, в том числе переводов денежных средств	Применение протоколов идентификации и аутентификации клиентов финансовой организации*
Формирование (подготовка), передача и прием электронных сообщений	Проверка правильности формирования (подготовки) электронных сообщений (двойной контроль)
	Проверка правильности заполнения полей электронного сообщения и прав владельца электронной подписи (входной контроль)
	Контроль дублирования электронных сообщений
	Структурный контроль электронных сообщений
	Защита защищаемой информации при ее передаче по каналам связи
Удостоверение права клиентов финансовой организации распоряжаться денежными средствами, ценными бумагами и иным имуществом	Подписание клиентом финансовой организации электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом**
	Получение от клиента финансовой организации подтверждения совершенной финансовой (банковской) операции
Осуществление финансовой (банковской) операции, учет результатов ее осуществления	Проверка соответствия (сверка) выходных электронных сообщений с входными электронными сообщениями
	Проверка соответствия (сверка) результатов осуществления финансовых (банковских) операций с информацией, содержащейся в электронных сообщениях
	Направление клиентам финансовой организации уведомлений об осуществлении финансовых (банковских) операций, в том числе переводов денежных средств, в том случае, когда такое уведомление предусмотрено законодательством Российской Федерации или договором
Хранение электронных сообщений и информации об осуществленных финансовых (банковских) операциях, в том числе переводах денежных средств	—

* Например, приведенных в [38], [39].

** Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, должно быть осуществлено в соответствии со статьей 6 Федерального закона [40].

Приложение Б
(обязательное)

Целевые показатели операционной надежности

Б.1 Базовый состав целевых показателей операционной надежности, определяемый нормативными актами Банка России [7], [8], приведен в таблице Б.1.

Б.2 В целях контроля за соблюдением установленных целевых показателей операционной надежности финансовая организация определяет сигнальные и контрольные значения для каждого целевого показателя операционной надежности. В рамках таблицы Б.1 применяют следующие обозначения:

- С — для сигнальных и контрольных значений целевых показателей операционной надежности, которые финансовая организация определяет самостоятельно (если иное не предусмотрено нормативными актами Банка России);
- ТН — для сигнальных и контрольных значений целевых показателей операционной надежности, которые кредитная организация определяет согласно требованиям нормативных актов Банка России.

Таблица Б.1

Контрольный показатель уровня риска	Сигнальное значение	Контрольное значение
1 Допустимая доля деградации каждого из бизнес- и технологического процессов	С	С
2 Допустимое время простоя и (или) деградации каждого из бизнес- и технологического процессов (в случае превышения допустимой доли деградации каждого из бизнес- и технологического процессов)*	С	ТН**
3 Допустимое суммарное время простоя и (или) деградации каждого из бизнес- и технологического процессов финансовой организации (в случае превышения допустимой доли деградации каждого из бизнес- и технологического процессов) в течение последних 12 календарных месяцев к первому числу календарного месяца*	С	С
4 Показатель соблюдения режима работы (функционирования) каждого из бизнес- и технологического процессов (времени начала, времени окончания, продолжительности и последовательности процедур в рамках каждого из бизнес- и технологического процессов)	С	С

* Допустимое суммарное время простоя и (или) деградации — предельно допустимый для финансовой организации суммарный временной период в течение 12 календарных месяцев, исчисляемых с первого числа каждого календарного месяца, в течение которого происходят инциденты (в случае превышения допустимой доли деградации каждого из бизнес- и технологического процессов).

При определении времени простоя и (или) деградации бизнес- и технологических процессов в расчет не включаются периоды времени проведения плановых технологических операций, связанных с приостановлением (частичным приостановлением) бизнес- и технологических процессов и проводимых в соответствии с внутренними документами финансовой организации.

** В отношении каждого из бизнес- и технологического процессов, обеспечивающего осуществление переводов денежных средств по распоряжениям участников платежной системы, пороговые значения показателя определяют в соответствии с нормативным актом Банка России [10].

Библиография

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

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

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

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

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

[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 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности»

[7] Нормативный акт Банка России, устанавливающий обязательные для кредитных организаций требования к операционной надежности при осуществлении банковской деятельности в целях обеспечения непрерывности оказания банковских услуг на основании статьи 57.5 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

[8] Нормативный акт Банка России, устанавливающий обязательные для некредитных финансовых организаций требования к операционной надежности при осуществлении деятельности в сфере финансовых рынков в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг) на основании статьи 76.4-2 Федерального закона от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»

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

[10] Нормативный акт Банка России, устанавливающий требования 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»

[11] 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)»

[12] 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)»

[13] 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»

[14] 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)»

[15] Письмо Банка России от 29 июня 2012 г. № 94-Т «О документе Комитета по платежным и расчетным системам «Принципы для инфраструктур финансового рынка»

[16] «Методические рекомендации по обеспечению непрерывности деятельности некредитных финансовых организаций» (утверждены Банком России 18 августа 2016 г. № 28-МР)

[17] «Методические рекомендации по обеспечению непрерывности деятельности системно значимых инфраструктурных организаций финансового рынка» (утверждены Банком России 27 июля 2015 г. № 20-МР)

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

[19] 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»

[20] 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»

[21] ИСО/МЭК 19510:2013 Информационные технологии. Модель и нотация процесса менеджмента объекта в групповом бизнесе (Information technology — Object Management Group Business Process Model and Notation)

[22] TOGAF® Standard. URL: gost.e-ecolog.ru (дата обращения 27 августа 2020 г.)

[23] 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 publ/d146.pdf (дата обращения: 10 апреля 2021 г.)

[24] ITIL® Foundation ITIL 4 Edition

[25] COBIT® 2019 Framework: Governance and Management Objectives

[26] Common Vulnerabilities and Exposures (CVE®). URL: gost.e-ecolog.ru (дата обращения: 21 августа 2020 г.)

[27] Банк данных угроз безопасности информации. URL: gost.e-ecolog.ru (дата обращения: 21 августа 2020 г.)

[28] The Financial Stability Board. Effective Practices for Cyber Incident Response and Recovery. Consultative Document. URL: gost.e-ecolog.ru .pdf (дата обращения: 10 апреля 2021 г.)

[29] ИСО/МЭК 27035-1—2016 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 1. Принципы менеджмента инцидентов (Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management)

[30] ИСО/МЭК 27035-2—2016 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. Часть 2. Руководящие указания по планированию и разработке реагирования на инциденты (Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response)

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

[32] 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

[33] Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также порядок реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента на основании частей 4, 6 и 7 статьи 27 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[34] Нормативный акт Банка России, устанавливающий формы и порядок направления операторами по переводу денежных средств уведомлений о приостановлении зачисления денежных средств на банковский счет получателя средств или увеличения остатка электронных денежных средств получателя средств, о невозможности приостановления зачисления денежных средств на банковский счет получателя средств или приостановления увеличения остатка электронных денежных средств получателя средств на основании частей 11.1 и 11.5 статьи 9 Федерального закона от 27 июня 2011 г. № 161-ФЗ «О национальной платежной системе»

[35] 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

[36] ИСО/МЭК 27036-3—2013 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий (Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security)

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

[38] FIDO Alliance Proposed Standard. Universal 2nd Factor (UAF) Overview. URL: gost.e-ecolog.ru gost.e-ecolog.ru (дата обращения 10 апреля 2021 г.)

[39] FIDO Alliance Proposed Standard. Universal Authentication Framework (UAF) Architectural Overview. URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html (дата обращения: 13 апреля 2021 г.)

[40] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

УДК 004.056.5:006.354 ОКС 03.060 35.030

Ключевые слова: обеспечение операционной надежности, система обеспечения операционной надежности, система организации и управления операционной надежностью, уровень защиты, требования к системе обеспечения операционной надежности, требования к системе организации и управления операционной надежностью

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *М.И. Першина*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 23.12.2022. Подписано в печать 19.01.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,51. Уч.-изд. л. 5,86.

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