ПАРТАД

Типовой регламент защиты информации и операционной надежности некредитной финансовой организации

2023

ОДОБРЕНО
Комитетом ПАРТАД по ВКВАУР
Протокол № 1/2023 от 27.01.2023г.
С изменениями
Протокол №2/2023 от 06.04.2023г.

Типовой регламент

защиты информации и операционной надежности некредитной финансовой организации

г. Москва, 202_ г.

Содержание

1. Общие положения

1.1. Настоящий Регламент защиты информации и операционной надежности (далее – Регламент) является внутренним документом_____, осуществляющего деятельность _____ (далее – Общество), устанавливающим порядок организации и обеспечения Обществом защиты информации в рамках управления риском реализации информационных угроз, в том числе в целях обеспечения операционной надежности и непрерывности оказания финансовых услуг.

1.2. Настоящий Регламент разработан в соответствии с требованиями Банка России к обеспечению защиты информации[1] и операционной надежности[2] некредитной финансовой организации (далее - НФО) в рамках сформированных Обществом систем управления рисками и внутреннего контроля.

1.3. Термины и определения.

База данных о рисках – информационная база, реализованная программными средствами, обеспечивающая пользователя полным спектром связанной информации, как по отдельным рискам (включая риски реализации информационных угроз), так и по системе управления рисками Общества в целом.

Бизнес-процесс – набор взаимосвязанных операций, в том числе технических, в отношении активов финансовой организации или информации и (или) объектов информатизации, используемых при осуществлении финансовой организацией видов деятельности, связанных с предоставлением финансовых и (или) информационных услуг[3].

Деградация технологического процесса – нарушения технологического процесса, приводящие к неоказанию или ненадлежащему оказанию финансовых услуг, в том числе к простою в реализации технологического процесса.

Информация – сведения о лицах, предметах, фактах, событиях, процессах и явлениях независимо от формы их представления.

Информационная безопасность (ИБ) - защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения

[1] Положение Банка России от 20 апреля 2021 года №757-П «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций» (далее - Положение 757-П)

[2] Положение Банка России от 15 ноября 2021 года №779-П «Об установлении обязательных для некредитных финансовых организаций требований к операционной надежности при осуществлении видов деятельности, предусмотренных частью первой статьи 76[1] Федерального закона от 10 июля 2002 года №86-ФЗ «О Центральном банке Российской Федерации (Банке России)», в целях обеспечения непрерывности оказания финансовых услуг (за исключением банковских услуг)» (далее - Положение 779-П)

[3] Согласно п. 3.1 ГОСТ 57580.3-2022

конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

Информационная инфраструктура (ИИ) – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам[1].

Информационные угрозы - угрозы, приводящие к реализации риска информационной безопасности (киберриска), т.е. угрозы безопасности информации[2].

Информационные ресурсы – информация о лицах, фактах, событиях, процессах и явлениях в сфере профессиональной и хозяйственно-финансовой деятельности Общества, включенная в систему обработки информации, или являющиеся ее результатом в различных формах представления на различных носителях, используемая (необходимая) в деятельности Общества, доступ к которой регламентируется правилами разграничения доступа.

Инциденты защиты информации – рисковые события, связанные с обеспечением защиты информации / реализацией информационной угрозы при осуществлении деятельности в сфере финансовых рынков.

Инциденты операционной надежности – события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг.

Критичная архитектура – совокупность следующих элементов организации деятельности Общества:

технологические процессы и их участки, реализуемые непосредственно Обществом;

подразделения (работники) Общества, ответственные за разработку технологических процессов, реализуемых Обществом;

объекты информационной инфраструктуры Общества, задействованные при исполнении технологических процессов, реализуемых непосредственно Обществом;

технологические процессы, указанные в п.3.1 настоящего Регламента, технологические участки технологических процессов, реализуемых внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов (поставщики услуг);

работники Общества или иные лица, осуществляющие физический и (или) логический доступ, или программные сервисы, осуществляющие логический доступ к объектам информационной инфраструктуры Общества (субъекты доступа), задействованные при выполнении технологических процессов;

взаимосвязи и взаимозависимости между Обществом и иными НФО, кредитными

[1] ГОСТ Р 53114-2008 Национальный стандарт РФ. Обеспечение информационной безопасности в организации. Основные термины и определения.

[2] Письмо Банка России «О вопросах применения Положения Банка России № 779-П» №56-27/1045 от 24.08.2022

организациями (далее - КО) и поставщиками услуг в рамках выполнения технологических процессов Общества;

каналы передачи защищаемой информации, указанной в пункте 1.1 Положения Банка России от 20 апреля 2021 года №757-П, обрабатываемой и передаваемой в рамках технологических процессов его участниками.

Объекты информационной инфраструктуры – совокупность объектов и ресурсов доступа, средств и систем обработки информации, используемых для обеспечения информатизации бизнес- и технологических процессов Общества, используемых для предоставления финансовых и (или) информационных услуг[1].

Объекты информатизации - см. объекты информационной инфраструктуры.

Объекты доступа – объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав автоматизированных систем Общества, задействованный при выполнении технологических процессов Общества, а также информационный ресурс, доступ к которому регламентирован правилами разграничения доступа.

Поставщики услуг в сфере информационных технологий – третьи лица (внешние подрядчики, контрагенты, спецдепозитарии, КО и др.), оказывающие услуги в сфере информационных технологий, связанные с выполнением технологических процессов.

События операционного риска, связанные с нарушением операционной надежности – см. инцидент операционной надежности.

Система управления рисками (СУР) – совокупность процессов, мероприятий, методик, информационных систем, направленных на достижение целей и задач управления рисками.

Система внутреннего контроля (СВК) – комплекс мероприятий, осуществляемых Обществом в целях контроля за соответствием его деятельности требованиям законодательства Российской Федерации, нормативных актов Банка России, базовых и внутренних стандартов саморегулируемой организации в сфере финансового рынка, членом которой является Общество, учредительных и внутренних документов Общества.

Субъекты доступа – работники Общества или иные лица, осуществляющие физический и (или) логический доступ в соответствии с требованиями настоящего Регламента, или программные сервисы, осуществляющие логический доступ к объектам информационной инфраструктуры и информационным ресурсам Общества, задействованные при выполнении каждого технологического процесса.

Технологический процесс – процесс, реализуемый Обществом с использованием критичной архитектуры, определенный в соответствии с Приложением к Положению Банка России от 15

[1] Согласно п.3.2. ГОСТ 57580.3-2022

ноября 2021 года №779-П.

Показатели операционной надежности – предельные / пороговые и фактические значения индикаторов риска реализации информационных угроз в отношении операционной надежности.

В отношении иных терминов, определения которых не содержатся в настоящем Регламенте, используются понятия и термины, содержащиеся в нормативных правовых актах Российской Федерации, нормативных актах Банка России, регламентирующих осуществление профессиональной деятельности Общества на финансовом рынке, а также в иных внутренних документах Общества.

2. Обеспечение защиты информации

2.1. В целях противодействия осуществлению незаконных финансовых операций при осуществлении деятельности_____ Общество обеспечивает защиту следующей информации, получаемой, подготавливаемой, обрабатываемой, передаваемой и хранимой в информационной инфраструктуре Общества (далее – информация):

- информации, содержащейся в документах, составляемых при осуществлении финансовых операций в электронном виде работниками Общества и (или) клиентами Общества (далее - электронные сообщения);
- информации, необходимой Обществу для авторизации своих клиентов в целях осуществления финансовых операций и удостоверения прав клиентов распоряжаться денежными средствами, ценными бумагами или иным имуществом;
- информации об осуществленных Обществом и его клиентами финансовых операциях;
- ключевой информации средств криптографической защиты информации (далее – СКЗИ), используемой Обществом и его клиентами при осуществлении финансовых операций (далее – криптографические ключи).

В случае, если защищаемая информация содержит персональные данные, Обществом применяются меры[1] по обеспечению безопасности персональных данных при их обработке.

2.2. Обеспечение защиты информации с помощью средств криптографической защиты информации осуществляется Обществом в соответствии с технической документацией на СКЗИ, а также:

- Федеральным законом от 6 апреля 2011 года №63-ФЗ «Об электронной подписи»;
- Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных»;

[1] В соответствии со статьей 19 Федерального закона от 27 июля 2006 года N 152-ФЗ "О персональных данных"

- постановлением Правительства Российской Федерации от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
- приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года №378 «Об утверждении Состава и содержания 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».

2.3. При наличии в технической документации на СКЗИ требований к оценке влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявляемых к ним требований, Общество проводит указанную оценку в соответствии с Положением ПКЗ-2005, по техническому заданию, согласованному с федеральным органом исполнительной власти в области обеспечения безопасности.

При применении Обществом СКЗИ российского производства применяются СКЗИ, имеющие сертификаты соответствия федерального органа исполнительной власти в области обеспечения безопасности, безопасность процессов изготовления которых обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

2.4. Обществом осуществляется защита информации в отношении эксплуатируемых автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (объектов информационной инфраструктуры) в соответствии с требованиями ГОСТ Р 57580.1-2017[1], который применятся по результатам определения Обществом реализуемого в течение календарного года уровня защиты информации, предусмотренного ГОСТ Р 57580.1-2017.

Определение уровня защиты информации осуществляется Обществом ежегодно не позднее десятого рабочего дня календарного года.

[1] Национальный стандарт Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года №822-ст «Об утверждении национального стандарта Российской Федерации»

2.5. В соответствии с критериями[1] определения реализуемого в течение календарного года уровня защиты информации Обществом реализуется _____уровень защиты информации.

При реализации минимального уровня защиты информации Общество самостоятельно определяет необходимость сертификации[2] или оценки соответствия[3] прикладного программного обеспечения автоматизированных систем и приложений.

По решению Общества оценка соответствия прикладного программного обеспечения автоматизированных систем и приложений проводится самостоятельно или с привлечением проверяющей организации[4].

Признание электронных сообщений, подписанных электронной подписью, равнозначными документам на бумажном носителе, подписанным собственноручной подписью, осуществляется в соответствии со статьей 6 Федерального закона «Об электронной подписи».

2.6. Обществом обеспечивается доведение до своих клиентов рекомендаций по защите информации от воздействия программных кодов, приводящего к нарушению штатного функционирования средства вычислительной техники (вредоносного кода), в целях противодействия незаконным финансовым операциям.

Обществом также обеспечивается доведение до своих клиентов:

- информации о возможных рисках несанкционированного доступа к защищаемой информации с целью осуществления финансовых операций лицами, не обладающими правом их осуществления;
- информации о мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) клиентом устройства, с использованием которого им совершались действия в целях осуществления финансовой операции, контролю конфигурации устройства, с использованием которого клиентом совершаются действия в целях осуществления финансовой операции, и своевременному обнаружению воздействия вредоносного кода.

2.7. Обществом в соответствии с документами системы управления рисками (далее – СУР) осуществляется выявление инцидентов защиты информации, представление сведений о выявленных инцидентах защиты информации лицу, ответственному за организацию управления

[1] Установленными в п.1.4.4 Положения 757-П

[2] В системе сертификации Федеральной службы по техническому и экспортному контролю

[3] В соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 ноября 2013 года № 1340-ст "Об утверждении национального стандарта"

[4] Сторонней организации, имеющей лицензию на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года № 79 "О лицензировании деятельности по технической защите конфиденциальной информации"

рисками в Обществе (далее - _____), а также регистрация инцидентов защиты информации путем внесения информации в базу данных по рискам.

При этом к инцидентам защиты информации Обществом относятся рисковые события, которые привели или, по оценке _____, могут привести к осуществлению финансовых операций без согласия (волеизъявления) клиента Общества, неоказанию услуг, связанных с осуществлением финансовых операций, в том числе события, включенные в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в сети «Интернет».

В отношении каждого инцидента защиты информации Обществом фиксируется результат реагирования на него, в том числе совершенных действий по возврату денежных средств, ценных бумаг или иного имущества клиента Общества.

2.8. Обществом осуществляется информирование Банка России:

- о выявленных инцидентах защиты информации, включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и размещаемый Банком России на своем официальном сайте в сети «Интернет», а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный Обществом или Банком России инцидент защиты информации;
- о принадлежащих Обществу и (или) администрируемых в его интересах сайтах в сети «Интернет», которые используются Обществом для осуществления деятельности в сфере финансовых рынков;
- о планируемых Обществом мероприятиях, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на официальных сайтах Общества в сети «Интернет», в отношении инцидентов защиты информации не позднее одного рабочего дня до дня проведения мероприятия.

2.9. Сведения, указанные в п.2.8 настоящего Регламента, предоставляются Обществом в Банк России с использованием технической инфраструктуры (автоматизированной системы) Банка России. В случае технической невозможности взаимодействия Общества с Банком России с использованием технической инфраструктуры (автоматизированной системы) Банка России Общество предоставляет в Банк России сведения с использованием резервного способа взаимодействия[1].

[1] Информация о технической инфраструктуре (автоматизированной системе) Банка России, резервном способе взаимодействия, форме и сроках направления сведений размещается на официальном сайте Банка России в сети "Интернет"

3. Обеспечение операционной надежности

3.1. Обществом обеспечивается операционная надежность при осуществлении деятельности _____с использованием информационной инфраструктуры в отношении следующих технологических процессов:

- _____;
- _____;
- _____.

3.2. В рамках соблюдения требований операционной надежности Обществом обеспечивается непревышение пороговых / предельных значений показателей, указанных в **Приложении 1**[1] к настоящему Регламенту:

- допустимого времени простоя технологических процессов, указанных в п.3.1 настоящего Регламента

и (или)

- допустимого времени деградации технологических процессов – нарушения технологических процессов, указанных в п.3.1 настоящего Регламента, приводящего к неоказанию или ненадлежащему оказанию Обществом финансовых услуг.

3.3. В рамках обеспечения операционной надежности Обществом для каждого технологического процесса, осуществляемого Обществом, в рамках его СУР и СВК в соответствии с настоящим Регламентом рассчитывается (**Приложение 2** к настоящему Регламенту) и контролируется соблюдение пороговых / предельных значений следующих показателей операционной надежности:

- доли деградации технологических процессов – допустимого отношения общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг, к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг;
- допустимого времени простоя и (или) деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса), не выше предельного уровня, установленного Обществом;
- допустимого суммарного времени простоя и (или) деградации технологического процесса

[1] установленных согласно приложению к Положению 779-П Банка России в разрезе видов деятельности на финансовом рынке

(в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца;

- показателя соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).

В случае превышения допустимой доли деградации технологических процессов Общество обеспечивает фиксацию:

- фактического времени простоя и (или) деградации технологического процесса, исчисляемого по каждому событию операционного риска, связанному с нарушением операционной надежности (с момента нарушения технологического процесса по причине реализации события операционного риска, связанного с нарушением операционной надежности, до момента восстановления выполнения технологического процесса);

- фактической доли деградации технологического процесса, исчисляемой по каждому событию операционного риска, связанному с нарушением операционной надежности;

- суммарного времени простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев, предшествующих событию операционного риска, связанному с нарушением операционной надежности.

Указанные выше показатели операционной надежности, кроме показателя соблюдения режима работы, являются ключевыми индикаторами риска (КИР) и к ним применяются правила, установленные документами СУР Общества.

При достижении предельного значения КИР _____ совместно с подразделениями первой «линии защиты» Общества, ответственными за реализацию соответствующих технологических процессов, разрабатывает мероприятия / меры по минимизации операционного риска, связанного с операционной надежностью, которые представляются на утверждение _____ Общества.

Параметры показателя соблюдения режима работы определяются в рамках учета и контроля состояния критичной архитектуры. При нарушении данного показателя проводится идентификация и классификация риска в порядке, определенном документами СУР, а информация о рисковом событии и о мерах реагирования на него вносится в базу данных о рисках.

Обществом обеспечивается контроль за соблюдением предельных значений показателей операционной надежности.

3.4. Обществом не реже одного раза в год проводится анализ необходимости пересмотра предельных значений показателей операционной надежности, по итогам которого они либо пересматриваются, либо принимается мотивированное решение об отсутствии необходимости в пересмотре указанных значений.

3.5. Обществом в рамках обеспечения операционной надежности обеспечивается организация учета и контроля следующих элементов критичной архитектуры (при их наличии):

- технологических процессов, указанных в п.3.1 настоящего Регламента, реализуемых непосредственно Обществом;
- подразделений (работников) Общества, ответственных за разработку технологических процессов, указанных в п.3.1 настоящего Регламента, поддержание их выполнения и их реализацию;
- объектов информационной инфраструктуры Общества, задействованных при выполнении каждого технологического процесса, указанного в п.3.1 настоящего Регламента, реализуемого непосредственно Обществом;
- технологических участков технологических процессов указанных в п.3.1 настоящего Регламента, реализуемых непосредственно Обществом;
- технологических участков технологических процессов, указанных в п.3.1 настоящего Регламента, реализуемых поставщиками услуг – внешними контрагентами, оказывающими услуги в сфере информационных технологий, связанные с выполнением технологических процессов;
- субъектов доступа, задействованных при выполнении каждого технологического процесса, указанного в п.3.1 настоящего Регламента;
- взаимосвязей и взаимозависимостей между Обществом и иными участниками технологического процесса – НФО, КО и поставщиками услуг в рамках выполнения технологических процессов, указанных в п.3.1 настоящего Регламента;
- каналов передачи защищаемой информации, указанной в пункте 2.1 настоящего Регламента, обрабатываемой участниками технологического процесса и передаваемой в рамках технологических процессов, указанных в п.3.1 настоящего Регламента.

3.6. Порядок ведения учета элементов критичной архитектуры и структура учета определены в **Приложении 3** к настоящему Регламенту.

3.7. В случае отнесения элементов критичной архитектуры Общества к значимым объектам критической информационной инфраструктуры[1] Обществом будут выполнены требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры[2].

3.8. В рамках обеспечения операционной надежности Обществом выполняются следующие требования в отношении управления изменениями критичной архитектуры:

- управление уязвимостями в критичной архитектуре, с использованием которых могут реализоваться информационные угрозы и которые могут повлечь отклонение от значений

[1] В соответствии с пунктом 3 статьи 2 Федерального закона от 26 июля 2017 года №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Федеральный закон от 26 июля 2017 года №187-ФЗ)

[2] Установленные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 года №187-ФЗ

показателей операционной надежности, указанных в п.3.3 настоящего Регламента;

- планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение непрерывного оказания финансовых услуг;
- управление конфигурациями объектов информационной инфраструктуры Общества;
- управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры Общества.

Управление уязвимостями и управление конфигурациями в критичной архитектуре (в том числе в объектах информационной инфраструктуры) выполняется в порядке, установленном внутренними документами Общества по информационной безопасности.

Планирование и внедрение изменений в критичной архитектуре выполняется на основе качественной и/или количественной оценки операционного риска, проводимой в порядке, установленном документами СУР.

3.9. В рамках обеспечения защиты информации и операционной надежности Общества в отношении событий операционного риска, связанных с нарушением операционной надежности, Обществом обеспечивается следующее:

- выявление и регистрация событий операционного риска, связанных с нарушением операционной надежности;
- реагирование на события операционного риска, связанные с нарушением операционной надежности, в отношении критичной архитектуры;
- восстановление выполнения технологических процессов и функционирования своих объектов информационной инфраструктуры после реализации событий операционного риска, связанных с нарушением операционной надежности;
- проведение анализа причин и последствий реализации событий операционного риска, связанных с нарушением операционной надежности;
- организация взаимодействия между подразделениями (работниками) Общества, ответственными за разработку технологических процессов, указанных в п.3.1 настоящего Регламента, поддержание их выполнения, их реализацию, между собой и Банком России, иными участниками технологического процесса в рамках реагирования на события операционного риска, связанные с нарушением операционной надежности, и восстановления выполнения технологических процессов, а также функционирования объектов информационной инфраструктуры после реализации событий операционного риска, связанных с нарушением операционной надежности.

Указанные действия осуществляются Обществом в порядке, установленном документами СУР.

3.10. В рамках обеспечения операционной надежности Обществом обеспечивается выполнение следующих требований в отношении взаимодействия с поставщиками услуг в сфере информационных технологий:

- управление ***риском реализации информационных угроз*** при привлечении внешних поставщиков информационных и программно-технических услуг, в том числе защита своих объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг;
- управление ***риском технологической зависимости*** функционирования своих объектов информационной инфраструктуры от поставщиков услуг (утрата данных, утрата доступа, доступ к информации третьих лиц).

Для определения целесообразности привлечения внешних поставщиков информационных и программно-технических услуг необходимо провести оценку возможных потерь по результатам реализации вышеперечисленных рисков и сопоставить с эффектом от реализации внешними поставщиками указанных услуг Обществу.

3.11. В рамках обеспечения защиты информации и операционной надежности Обществом предпринимаются организационные и технические меры, направленные на проведение сценарного анализа (в части возможной реализации информационных угроз) и тестирования с использованием его результатов своей готовности противостоять реализации информационных угроз в отношении критичной архитектуры.

3.12. В целях обеспечения защиты информации и операционной надежности Общество регламентирует доступ к объектам ИИ и информационным ресурсам работников Общества и работников поставщиков услуг, привлекаемых для выполнения технологических процессов Общества согласно требованиям, определенным в документах Общества по информационной безопасности.

3.13. В рамках обеспечения осведомленности об актуальных информационных угрозах, которые могут привести к инцидентам операционной надежности, Общество определяет следующий порядок взаимодействия Общества и иных участников технологического процессов при обмене информацией об актуальных сценариях реализации информационных угроз:

1. _____ осуществляет анализ сведений, полученных из ФинЦЕРТ Банка России и определяет применимость их для целей операционной надежности.

2. При возможной применимости сведений из ФинЦЕРТ Банка России к Обществу, _____ в целях обеспечения непрерывного оказания финансовых услуг инициирует мероприятия по минимизации операционного риска, связанного с операционной надежностью в порядке, определенном в документах СУР Общества.

3.14. В рамках обеспечения операционной надежности Обществом обеспечивается управление ***риском возникновения зависимости*** обеспечения операционной надежности от

субъектов доступа – работников Общества, обладающих знаниями, опытом и компетенцией, которые отсутствуют у всех иных работников Общества.

В целях управления риском возникновения зависимости обеспечения операционной надежности от ключевых работников Общество принимает такие меры, как:

• максимальная автоматизация и регламентация процессов, которая позволяет привлекать к их выполнению менее квалифицированный персонал и тратить меньше времени на его переподготовку;

• перераспределение обязанностей и выстраивание каждого бизнес-процесса таким образом, чтобы результат не зависел от одного работника;

• проведение регулярных обучающих мероприятий как внутри Общества, так и с привлечением сторонних организаций;

• использование института наставничества и подготовку кадрового резерва внутри Общества.

3.15. Обществом обеспечивается защита критичной архитектуры от возможной реализации информационных угроз в периоды или в случаях выполнения работниками Общества трудовых функций дистанционно согласно требованиям внутренних документов Общества по информационной безопасности.

3.16. Для целей выполнения требований к операционной надежности Общество определяет состав процедур, а также порядок организационного взаимодействия подразделений Общества (с учетом конфликта интересов), участвующих в обеспечении операционной надежности:

За непосредственную организацию (построение) и эффективную защиту информации в информационной инфраструктуре (далее - ИИ) Общества отвечают Уполномоченное лицо по информационной безопасности, функцию которого может на условиях аутсорсинга выполнять внешний поставщик соответствующих услуг.

Первая «линия защиты» от реализации рисков информационных угроз реализуется подразделениями Общества, непосредственно осуществляющими ввод и обработку информации в ИИ Общества в рамках технологических и бизнес-процессов деятельности _____ на финансовом рынке.

Общий контроль реализации настоящего Регламента на второй «линии защиты» осуществляет _____ Общества.

Мониторинг обеспечения защиты информации и операционной надежности в Обществе, включая оценку результативности мер управления рисками информационных угроз, осуществляется _____ Общества.

Уполномоченное лицо по информационной безопасности сочетает в себе функции первой и второй «линий защиты», являясь, с одной стороны, основным владельцем рисков реализации информационных угроз, а с другой - осуществляя контроль за соблюдением технических мер управления указанными рисками и применением соответствующих технических средств

сотрудниками и подразделениями Общества на первой «линии защиты». В этих своих ролях Уполномоченное лицо по информационной безопасности взаимодействует с _____, который определяет ключевые индикаторы рисков реализации информационных угроз, в том числе в виде показателей операционной надежности. Распределение основных функций органов управления и должностных лиц Общества, связанных с обеспечением защиты информации и операционной надежности, представлено в Таблице 1.

Таблица 1

Основные функции подразделений и должностных лиц Общества, связанные с обеспечением защиты информации и операционной надежности

Ответственное должностное лицо/подразделение	**Функции**

3.17. Общество осуществляет контроль за соблюдением требований к защите информации и операционной надежности в порядке, определенном в документах СВК Общества. Соответствующие базовые процедуры внутреннего контроля определены в **Приложении 4** к настоящему Регламенту.

3.18. Обществом обеспечивается реализация требований к защите информации и операционной надежности, начиная с разработки и планирования внедрения технологических процессов, указанных в п.3.1 настоящего Регламента.

3.19. В рамках обеспечения операционной надежности Обществом осуществляется:

- моделирование информационных угроз в отношении критичной архитектуры;
- планирование применения организационных и технических мер, направленных на реализацию требований к операционной надежности, на основе результатов оценки ***риска реализации информационных угроз,*** в рамках сформированной Обществом системы управления рисками;
- реализация требований к операционной надежности на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации своих объектов информационной инфраструктуры;
- контроль соблюдения требований к операционной надежности в отношении элементов

критичной архитектуры.

3.20. Обществом осуществляется регистрация событий операционного риска, связанных с нарушением операционной надежности, в порядке, установленном документами СУР Общества.

3.21. Общество ведет базу данных о рисках, в которой регистрируются события операционного риска, включая инциденты операционной надежности.

Событие операционного риска, является инцидентом операционной надежности при соблюдении всех следующих условий:

1) это событие операционного риска или с превышением допустимого уровня финансового ущерба, устанавливаемого согласно документам СУР Общества, или если потери/снижение качества услуг равны либо превышают (снижение качества оказываемых Обществом финансовых услуг) средний уровень (см. п.3.22 настоящего Регламента);
2) время, в течение которого произошло событие, соответствует времени реализации технологического процесса;
3) событие вызвано информационными угрозами и (или) сбоями в работе объектов информационной инфраструктуры;
4) событие привело к неоказанию или ненадлежащему оказанию финансовых услуг.

3.22. Обществом устанавливаются следующая шкала снижения качества оказываемых Обществом финансовых услуг от реализации инцидентов операционной надежности в случае, если они не определяются в денежном выражении для технологических процессов, обеспечивающих _____(таблица 2).

Таблица 2

Время приостановки технологического процесса	**Оценка уровня снижения качества услуг**

3.23. В случаях выявления инцидента операционной надежности Общество обеспечивает внесение следующей дополнительной информации в базу данных о рисках:

- фактическое время простоя и (или) деградации технологического процесса, исчисляемого по каждому инциденту операционной надежности (с момента нарушения технологического процесса, приводящего к неоказанию или ненадлежащему оказанию банковских услуг, в связи с

возникновением события или серии связанных событий, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, до момента восстановления технологического процесса);

- фактическое количество выполненных операций в рамках отдельного инцидента операционной надежности;
- ожидаемое количество выполненных операций в рамках отдельного инцидента операционной надежности;
- фактическая доля деградации технологического процесса в рамках отдельного инцидента операционной надежности;
- превышение фактической доли деградации технологического процесса над предельной долей его деградации;
- признак, является ли данное событие инцидентом операционной надежности;
- код типа инцидента операционной надежности согласно перечню типов, размещаемого Банком России в сети «Интернет».

При определении времени простоя и (или) деградации технологических процессов в расчет не включаются периоды времени плановых технологических процедур, связанных с приостановлением (частичным приостановлением) технологических процессов и проводимых в соответствии с внутренними документами Общества.

4. Меры, направленные на реализацию требований к защите информации и операционной надежности

4.1. Обществом предпринимаются следующие меры, направленные на реализацию требований Банка России к защите информации и операционной надежности:

4.1.1. Определение и описание состава процедур контроля за соблюдением мер обеспечения защиты информации и операционной надежности, содержащих следующую информацию (см. **Приложение 4**):

- наименование процедуры контроля;
- ответственный за проведение процедуры контроля.
- содержание процедуры контроля;
- периодичность / порядок проведения процедуры контроля;
- результат проведения процедуры контроля.

4.1.2. Определение подразделений и должностных лиц Общества, задействованных в выполнении требований к защите информации и операционной надежности, включающее:

– возложение на должностных лиц / подразделения Общества полномочий по контролю за соблюдением мер обеспечения защиты информации и операционной надежности (в том числе в части принятия решений, касающихся выполнения требований к операционной надежности), которые установлены в рамках СУР Общества;

– определение функций должностных лиц / подразделений Общества по реализации процедур контроля за соблюдением мер защиты информации и операционной надежности, определенных в рамках СВК[1].

4.1.3. Выделение ресурсного обеспечения, необходимого для выполнения Обществом требований к защите информации и операционной надежности согласно функциям, определенным в п.3.16 настоящего Регламента.

4.2. Процедуры контроля за соблюдением мер обеспечения защиты информации и операционной надежности разрабатываются _____ совместно с _____ и утверждаются _____ Общества.

4.3. Общество пересматривает меры обеспечения защиты информации и операционной надежности и контрольные процедуры, направленные на их соблюдение, по мере необходимости, в том числе при изменении требований к операционной надежности НФО, установленных законодательством Российской Федерации, нормативными актами Банка России, базовыми и внутренними стандартами саморегулируемой организации в сфере финансового рынка, членом которой является Общество.

5. Заключительные положения

5.1. Настоящий Регламент и изменения к нему утверждаются _____ Общества.

5.2. Общество пересматривает Регламент по мере необходимости, в том числе при изменении требований к защите информации и операционной надежности НФО, установленных законодательством Российской Федерации, нормативными актами Банка России, базовыми и внутренними стандартами саморегулируемой организации в сфере финансового рынка, членом которой является Общество.

5.3. В случае выявления каких-либо несоответствий Регламента требованиям к защите информации и операционной надежности НФО, установленных законодательством Российской Федерации, нормативными актами Банка России, базовыми и внутренними стандартами саморегулируемой организации в сфере финансового рынка, членом которой является Общество, а

[1] При наличии требований к системе внутреннего контроля, установленных законодательством Российской Федерации, нормативными актами Банка России, базовыми и внутренними стандартами саморегулируемой организации в сфере финансового рынка, членом которой является Общество

также иными документам Общества, Обществом осуществляется внесение изменений и дополнений в Регламент в целях устранения выявленных несоответствий.

5.4. Общество осуществляет хранение утративших силу редакций настоящего Регламента не менее 5 (пяти) лет с даты утверждения новой редакции.

Приложение 1
к Регламенту защиты информации и операционной надежности

_____

Показатели уровней операционного риска, связанных с нарушением операционной надежности за _____
(период)

№	Наименование технологического процесса (ТП)[1]	Код ТП	Ключевые индикаторы риска (КИР)						Показатели соблюдения режима работы (функционирования) ТП			
			Доля деградации ТП		Время простоя и (или) деградации ТП (мин)		Суммарное время простоя и (или) деградации ТП (мин)		время начала ТП	время окончания ТП	продолжительность ТП за период, час	
			допустимая/ предельная	фактическая[2]	допустимое/ предельное	фактическое[3]	допустимое/ предельное	фактическое			план	факт
1.												
2.												
3.												

[1] в соответствии с п.3.1 настоящего Регламента
[2] Под фактическим значением показателя «доля деградации ТП» в соответствии с принятой в СУР Общества политикой может пониматься один из следующих показателей:
- перечисление долей деградации ТП по всем инцидентам операционной надежности за период;
- средний уровень деградации ТП во время инцидентов операционной надежности произошедших за период;
-количество инцидентов операционной надежности в рамках ТП во время которых предельный уровень деградации не был соблюден.
[3] Под фактическим значением показателя «время простоя и (или) деградации ТП» в соответствии с принятой в СУР Общества политикой понимается один из следующих показателей:
- перечисление продолжительности простоев и (или) деградации ТП во время всех инцидентов операционной надежности в рамках ТП за период.
- среднее время простоя и (или) деградации ТП во время инцидентов операционной надежности за период.

Приложение 2
к Регламенту защиты информации
и операционной надежности

Порядок расчета показателей операционной надежности

1. Общество обеспечивает расчет предельных / пороговых и фактических значений показателей операционной надежности.

2. Набор показателей включает следующие:

- допустимая доля деградации - отношение общего количества финансовых операций, совершенных во время деградации технологического процесса в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами, которые привели к неоказанию или ненадлежащему оказанию финансовых услуг (далее - события операционного риска, связанные с нарушением операционной надежности), к ожидаемому количеству финансовых операций за тот же период в случае непрерывного оказания финансовых услуг (далее - доля деградации технологических процессов);
- допустимое время простоя и (или) деградации технологического процесса в рамках события операционного риска, связанного с нарушением операционной надежности (в случае превышения допустимой доли деградации технологического процесса), не выше порогового уровня, установленного в Приложении к Положению 779-П Банка России;
- допустимое суммарное время простоя и (или) деградации технологического процесса (в случае превышения допустимой доли деградации технологического процесса) в течение последних двенадцати календарных месяцев к первому числу каждого календарного месяца;
- показатель соблюдения режима работы (функционирования) технологического процесса (времени начала, времени окончания, продолжительности и последовательности процедур в рамках технологического процесса).

3. **Расчет показателя «Допустимая доля деградации»**

3.1. Предельное значение показателя «допустимая доля деградации» определяется в экспертном заключении с учетом допущения неоказания услуг, связанного с информационными угрозами. Предельное значение показателя определяется в долях единицы с точностью до 6 знаков после запятой (например, 0,988132). При формировании показателя следует ориентироваться на количество клиентов, которым услуга будет не оказана или оказана

ненадлежащим образом и на количество операций, которые не будут выполнены (например, 100 клиентов, 2000 операций). При формировании экспертного заключения необходимо использовать статистические данные не менее чем за 1 прошедший год.

3.2. Фактическое значение показателя «допустимая доля деградации» или фактическая доля деградации считается по формуле:

Кво/Коп, где:

Кво – количество совершенных операций в период реализации инцидента операционной надежности.

Коп – «плановое» / ожидаемое количество операций, соответствующее количеству совершенных в течение предшествующего сопоставимого периода.

Например, предшествующий период определяется как соответствующий период на прошлой неделе. В этом случае, при попадании предшествующего периода на выходной или праздничный день берется предыдущая неделя, перед праздничной, внутри которой выбирается период сопоставимый (по дням недели, часам и т.д.) с периодом, в рамках которого произошел инцидент операционной надежности.

4. **Расчет показателя «Допустимое время простоя».**

4.1. Предельное значение показателя «допустимое время простоя» определяется как предельный размер допустимого времени простоя, согласно Приложению к Положению 779-П Банка России. Экспертное заключение не оформляется, расчет не проводится.

4.2. Фактическое значение показателя «допустимое время простоя» или фактическое время простоя считается сразу после проведения идентификации и классификации рискового события по следующим условиям:

1. Рисковое событие является инцидентом операционной надежности.

2. Фактическое значение доли деградации превышает предельное значение показателя «допустимая доля деградации».

Расчет проводится в минутах, от начала действия события операционного риска до его окончания.

5. **Расчет показателя «Допустимое суммарное время простоя».**

5.1. Предельное значение показателя «допустимое суммарное время простоя» определяется экспертным путем.

5.2. Фактическое значение показателя «допустимое суммарное время простоя» или фактическое время простоя считается ежемесячно до 15 числа следующего месяца по следующим условиям:

1. Производится выборка инцидентов операционной надежности за последние двенадцать календарных месяцев, исчисляемых с первого числа каждого календарного месяца.

2. Из выборки исключаются инциденты, по которым не было превышения доли деградации.

3. Суммируется время всех оставшихся инцидентов.

Показатель считается в минутах.

6. **Показатель соблюдения режима работы** (функционирования) технологического процесса не является ключевым индикатором риска.

При нарушении данного показателя формируется сообщение о рисковом событии, проводится идентификация и классификация возможного риска в порядке, определенном в документах СУР Общества.

Приложение 3
к Регламенту защиты информации
и операционной надежности

Порядок ведения учета элементов критичной архитектуры

1. Общество выделяет следующие верхнеуровневые элементы критичной архитектуры:
   - субъекты доступа;
   - технологические процессы и участки;
   - бизнес-процессы;
   - информационные системы;
   - программно-технические средства;

2. Учет субъектов доступа.

2.1. Субъекты доступа учитываются в рамках реализации требований порядка доступа к информационным ресурсам / информационной инфраструктуре Общества.

3. Учет технологических процессов и участков технологических процессов.

3.1 Технологические процессы (ТП) учитываются в соответствующих учетных регистрах Общества с использованием следующих кодов:

Код ТП	**Расшифровка кода**
ТПрНФО…	
ТПрНФО…	
ТПрНФО…	

3.2. Реестр технологических процессов и участков технологических процессов ведется по форме Приложения 1 к настоящему Порядку.

4. Учет бизнес-процессов.

4.1. Реестр (список) бизнес-процессов определяется исполнительным органом Общества с учетом структуры управления Общества на основе предложений подразделений, ответственным за разработку и реализацию технологических процессов.

4.2. Каждый бизнес-процесс имеет ссылку на код технологического процесса, к которому он имеет отношение.

4.3. Реестр бизнес-процессов содержит в себе следующие учетные элементы:

- Дата начала действия процесса;
- Дата окончания действия процесса;
- Статус процесса (планируемый, действующий, исторический);
- Лицо (подразделение), ответственное за процесс;
- Описание процесса;
- Режим функционирования процесса (постоянно, периодически, разовый);
- Этапы процесса (последовательность процедур в рамках технологического процесса);
- Список направлений деятельности, в которых применяется процесс;
- Список подразделений, которые реализуют процесс;
- Объекты информатизации, используемые в рамках выполнения процесса;
- Субъекты доступа, работающие в рамках выполнения процесса;
- Указание на участие в реализации процесса внешнего поставщика услуг в сфере информационных технологий (в случае необходимости);
- Реквизиты внешнего поставщика услуг в сфере информационных технологий;
- Канал передачи защищаемой информации при взаимодействии с внешним поставщиком в сфере информационных технологий.

5. Учет информационных систем.

5.1. Общество ведет учет информационных систем (далее - ИС) в учетном регистре со следующими графами:

- Код ИС;
- Описание ИС, согласно требованиям Банка России[1];
- Дата начала эксплуатации ИС;
- Дата окончания эксплуатации ИС;
- Статус эксплуатации ИС (на согласовании, действует, не эксплуатируется);
- Объект доступа, на котором установлена ИС;
- Доменное имя ИС (если имеется);

[1] По мере формирования указанных требований

- Перечень защищаемой информация (ЗИ), обрабатываемой в ИС (с использованием нижеуказанным кодов):

Код ЗИ	Расшифровка кода
1	Авторизация клиентов
2	Криптографические ключи
3	Финансовые операции
4	Электронные сообщения

- Коды технологических участков (ТУ) реализуемых с использованием ИС:

Код ТУ	Расшифровка кода
ИАА	Идентификация, аутентификация и авторизация клиентов при совершении действий в целях осуществления финансовых операций и иных операций
ФПП	Формирование (подготовка), передача и прием электронных сообщений
УП	Удостоверение права клиентов распоряжаться денежными средствами и ценными бумагами
ОУ	Осуществление финансовой операции и иной операции, учет результатов ее осуществления
ХИ	Хранение электронных сообщений и информации об осуществленных финансовых операциях и иных операциях

- Признак участия в ИС внешних поставщиков ИТ-услуг (при наличии);
- Идентификационный код, присваиваемый Обществом центру обработки данных поставщика ИТ-услуг (при наличии);
- Уровень сертификации центра обработки данных (поставщика услуг (при наличии));
- Наличие SLA (Service Level Agreement) с внешним поставщиком услуг в сфере информационных технологий и его параметры;
- Функциональность (возможность), получаемая Обществом в случае применения облачных решений (ФОБР), с использованием следующих кодов:

Код ФОБР	Расшифровка кода
ФПр	Функциональность приложений (предоставляет Обществу возможность использовать приложения поставщика услуг облачных решений)
ФИИ	Функциональность информационной инфраструктуры (предоставляет Обществу возможность получать и использовать вычислительные ресурсы, ресурсы для хранения данных или сетевые ресурсы)
ФПл	Функциональность платформы (предоставляет Обществу возможность использовать приложения, созданные или приобретенные им, с использованием одного или нескольких языков программирования и одной или более сред выполнения, поддерживаемых поставщиком услуг облачных решений)

- Категория облачных решений (КОБР), в случае их предоставления поставщиком услуг, с использованием следующих кодов:

Код КОБР	Расшифровка кода
ОИ	Обмен информацией (категория, в которой Обществу предоставляются возможности, связанные с взаимодействием в реальном времени и совместной работой)
Вычисления	Вычисления (категория, в которой Обществу предоставляются возможности, связанные с получением и использованием вычислительных ресурсов, необходимых для развертывания и выполнения прикладного программного обеспечения)
ХД	Хранение данных (категория, в которой Обществу предоставляются возможности, связанные с предоставлением и использованием ресурсов для хранения данных)
ИИ	Информационная инфраструктура (категория, в которой Обществу предоставляются возможности, связанные с функциональностью информационной инфраструктуры)
Сеть	Сеть (категория, в которой Обществу предоставляются возможности, связанные с транспортной связностью, и связанные с ней сетевые возможности)
Платформа	Платформа (категория, в которой Обществу предоставляется возможности, связанные с функциональностью платформы)
ППО	Прикладное программное обеспечение (категория, в которой Обществу предоставляются возможности, связанные с функциональностью приложений)

БД	База данных (категория, в которой Обществу предоставляются возможности, связанные с функциональностью базы данных по требованию, где установка и обслуживание баз данных выполняются поставщиком услуг облачных решений)

6. Учет программно-технических средств.

6.1. Общество ведет учет программно-технических средств в учетном регистре со следующими графами:

- Код программно-технического средства (определяется Обществом самостоятельно);
- IP-адрес или пул IP-адресов в формате протокола IPv4 с указанием подсети в формате CIDR;
- IP-адрес или пул IP-адресов в формате протокола IPv6 с указанием с указанием префикса.

7. Общество определяет для каждого категории элементов критичной архитектуры лицо, ответственное за их учет:

Элементы критичной архитектуры	**Ответственное подразделение/лицо**
Субъекты доступа	
Технологические процессы и участки	
Бизнес-процессы	
Информационные системы	
Программно-технические средства	

Ответственные лица отслеживают изменения в рамках деятельности Общества и делают соответствующие записи в учетные регистры элементов критичной архитектуры.

Учет должен быть организован в соответствии с фактическим составом критичной архитектуры. Контроль за учетом элементов критичной архитектуры осуществляется уполномоченными должностными лицами Общества с использованием базовых процедур, определенных в **Приложении 4** к Регламенту защиты информации и операционной надежности.

Приложение 1
к Порядку ведению учета элементов
критичной архитектуры

Реестр
технологических процессов и технологических участков технологических процессов

№	**Технологические процессы (ТП)[1], реализуемые Обществом**	**Подразделения (работники) Общества, ответственные за разработку и реализацию ТП**	**Объекты информационной инфраструктуры Общества, задействованные при выполнении ТП**	**Технологические участки (ТУ) технологических процессов (ТП), реализуемых Обществом**	**Технологические процессы (ТП) (технологические участки ТП), реализуемые внешними поставщиками услуг**	**Субъекты доступа**	**Взаимосвязи и взаимозависимости с иными участниками ТП**	**Каналы передачи защищаемой информации[2]**
1.								
2.								
3.								

[1] указанный в приложении к Положению 779-П в разрезе видов деятельности на финансовом рынке
[2] указанной в п.2.1 настоящего Регламента

Приложение 4
к Регламенту защиты информации
и операционной надежности

Базовые процедуры внутреннего контроля (ПВК) за соблюдением мер защиты информации и обеспечения операционной надежности

№ п/п	Наименование процедуры внутреннего контроля	Ответственное лицо/подразделение	Содержание ПВК	Порядок реализации ПВК	Результат выполнения ПВК
1.	**Контроль учета субъектов доступа**	_____	1. Запросить у ответственного за ведение кадровой работы лица штатное расписание и у _____ информацию о субъектах доступа к ИИ / информационным ресурсам. 2. Получить в базе данных (при наличии ресурса доступа) либо запросить у _____ список субъектов доступа с ФИО пользователей и эксплуатационного персонала.	1.На этапе внедрения Регламента ЗИ и ОН. 2.Ежеквартально	1. Учетные записи пользователей и эксплуатационного персонала должны быть уникальны и персонифицированы. 2. Список субъектов доступа должен быть актуализирован.
2.	**Контроль учета технологических процессов и участков**	_____	1. Инициировать формирование _____ совместно с _____и подразделениями первой «линии защиты» реестра технологических процессов и участков. 2. Получить в базе данных (при наличии ресурса доступа) либо запросить у _____ реестр	1.На этапе внедрения Регламента ЗИ и ОН. 2.Ежеквартально	1.Реестр технологических процессов и участков должен быть сформирован. 2.Реестр технологических процессов и участков должен быть актуализирован

№ п/п	Наименование процедуры внутреннего контроля	Ответственное лицо/подразделение	Содержание ПВК	Порядок реализации ПВК	Результат выполнения ПВК
			технологических процессов и участков.		
3.	**Контроль учета бизнес-процессов**	_____	1. Инициировать формирование _____ и подразделениями первой «линии защиты» реестра (списка) бизнес-процессов. 2. Получить в базе данных (при наличии ресурса доступа) либо запросить у _____ реестр бизнес-процессов.	1.На этапе внедрения Регламента ЗИ и ОН. 2.Ежеквартально	1.Реестр бизнес-процессов должен быть сформирован. 2.Реестр бизнес-процессов должен быть актуализован.
4.	**Контроль учета информационных систем (ИС)**	_____	1. Проверить факт проведения инвентаризации ИС _____, актуальность ее результатов или, при необходимости, инициировать ее проведение. 2. Получить в базе данных (при наличии ресурса доступа) либо запросить у _____ перечень информационных систем.	1.На этапе внедрения Регламента ЗИ и ОН в случае, если она проводилась более года назад. 2.Ежеквартально	1. Перечень информационных систем должен быть сформирован. 2.Перечень должен быть актуализирован.
5.	**Контроль учета программно-технических средств (ПТС)**	_____	1. Проверить факт проведения инвентаризации ПТС _____, актуальность ее результатов или, при необходимости, инициировать ее проведение.	1. На этапе внедрения Регламента ЗИ и ОН.	1.Перечень ПТС должен быть сформирован.

№ п/п	Наименование процедуры внутреннего контроля	Ответственное лицо/подразделение	Содержание ПВК	Порядок реализации ПВК	Результат выполнения ПВК
			2. Получить в базе данных (при наличии ресурса доступа) либо запросить у _____ перечень ПТС.	2. Ежеквартально	2.Перечень ПТС должен быть актуализирован.
6.	**Контроль выявления инцидентов операционной надежности**	_____	Получить в базе данных по рискам (при наличии ресурса доступа) либо запросить у _____ перечень инцидентов операционной надежности за последний квартал.	Ежеквартально	Представленные данные должны быть проверены и сопоставлены с информацией из других источников.
7.	**Контроль расчета предельных значений показателей операционной надежности**	_____	Запросить у _____ расчет предельных значений показателей операционной надежности за соответствующий период.	Ежегодно	Соответствие установленному порядку расчета должно быть подтверждено.
8.	**Контроль за соблюдением предельных значений показателей операционной надежности**	_____	Получить в базе данных о рисках (при наличии ресурса доступа) либо запросить у _____ отчет по фактическим значениям показателей операционной надежности и информацию о реагировании на реализации риска информационных угроз.	Ежегодно / Ежеквартально	1.По каждому показателю операционной надежности, в отношении которого было превышено предельное значение, должно быть запланированы дополнительные меры управления рисками. 2.Запланированные меры управления рисками должны реализовываться в плановом порядке.