Проект

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)
П О Л О Ж Е Н И Е

«___» _____ 202_ г. №_____ -П

г. Москва

О требованиях к операционной надежности оператора автоматизированной информационной системы страхования

Настоящее Положение на основании подпункта 5 пункта 7 статьи 33.10 Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» устанавливает требования к операционной надежности, которые обязан соблюдать оператор автоматизированной информационной системы страхования.

1. Оператор автоматизированной информационной системы страхования (далее – оператор АИС страхования) должен соблюдать установленные настоящим Положением требования к операционной надежности с учетом требований к системе управления рисками (в части операционного риска), установленных нормативным актом Банка России, принятым на основании подпункта 8 пункта 7 статьи 33.10 Закона Российской Федерации от 27 ноября 1992 года № 4015-I «Об организации страхового дела в Российской Федерации» (далее – Закон Российской Федерации № 4015-I).

Требования к операционной надежности должны соблюдаться оператором АИС страхования при выполнении его функций с использованием автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее – объекты информационной инфраструктуры) в условиях реализации

информационных угроз и (или) возникновения отказов и (или) нарушений функционирования объектов информационной инфраструктуры и (или) несоответствия их функциональных возможностей и характеристик потребностям оператора АИС страхования (далее – сбои объектов информационной инфраструктуры).

2. Оператор АИС страхования должен обеспечить непревышение значения порогового уровня допустимого времени простоя и (или) нарушения технологических процессов, указанных в приложении к настоящему Положению (далее – технологические процессы), приводящих к невыполнению или ненадлежащему выполнению оператором АИС страхования своих функций (далее – пороговый уровень допустимого времени простоя и (или) деградации технологических процессов оператора АИС страхования), предусмотренного приложением к настоящему Положению.

3. Оператор АИС страхования должен определить во внутренних документах для каждого технологического процесса и соблюдать значения следующих контрольных показателей уровня операционного риска для целей обеспечения операционной надежности (далее – целевые показатели операционной надежности):

допустимого отношения общего количества операций, осуществляемых в рамках технологического процесса, совершенных во время нарушений технологических процессов, приводящих к невыполнению или ненадлежащему выполнению оператором АИС страхования своих функций (далее – деградация технологического процесса (технологических процессов), в рамках события операционного риска или серии связанных событий операционного риска, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, которые привели к невыполнению или ненадлежащему выполнению оператором АИС страхования своих функций (далее – инцидент операционной надежности), к ожидаемому количеству операций, осуществляемых в рамках технологических процессов, за тот же период в случае непрерывного

выполнения оператором АИС страхования своих функций, установленного оператором АИС страхования (далее – допустимая доля деградации технологического процесса);

допустимого времени простоя и (или) деградации технологических процессов оператора АИС страхования в рамках инцидента операционной надежности (в случае превышения допустимой доли деградации технологического процесса). Значение данного целевого показателя устанавливается оператором АИС страхования не выше значений, предусмотренных приложением к настоящему Положению;

допустимого суммарного времени простоя и (или) деградации технологического процесса оператора АИС страхования (в случае превышения допустимой доли деградации технологического процесса) в течение очередного календарного года;

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

Значение допустимой доли деградации технологических процессов должно рассчитываться оператором АИС страхования на основании статистических данных за период не менее двенадцати календарных месяцев, предшествующих дате определения значения целевого показателя операционной надежности, за исключением случая, предусмотренного абзацем седьмым настоящего пункта, и (или) иных данных, обосновывающих их определение (по выбору оператора АИС страхования).

В случае если технологический процесс функционирует менее двенадцати календарных месяцев, оператор АИС страхования должен определять 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 оператора АИС страхования).

4. В случаях превышения допустимой доли деградации технологических процессов оператор АИС страхования должен обеспечить фиксацию:

фактического времени простоя и (или) деградации технологического процесса, исчисляемого по каждому инциденту операционной надежности (с момента нарушения технологического процесса, приводящего к невыполнению или ненадлежащему выполнению оператором АИС страхования своих функций, в связи с возникновением события или серии связанных событий, вызванных информационными угрозами и (или) сбоями объектов информационной инфраструктуры, до момента восстановления технологического процесса);

фактической доли деградации технологического процесса в рамках отдельного инцидента операционной надежности;

суммарного времени простоя и (или) деградации технологического процесса за последние двенадцать календарных месяцев.

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

5. Оператор АИС страхования должен не реже одного раза в год проводить анализ необходимости пересмотра значений целевых показателей операционной надежности.

6. Оператор АИС страхования должен разработать во внутренних документах и выполнять требования к операционной надежности, которые включают в себя:

требования к порядку определения значений целевых показателей операционной надежности и обеспечению контроля за их соблюдением;

требования к идентификации состава совокупности элементов, указанных в подпункте 6.1 настоящего пункта (далее – критичная

арихтектура);

требования к управлению изменениями элементов, указанных в подпункте 6.1 настоящего пункта;

требования к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации указанных инцидентов;

требования к взаимодействию с третьими лицами (внешними подрядчиками, контрагентами), оказывающими на основании договора услуги в сфере информационных технологий, связанные с созданием, модернизацией, вводом в эксплуатацию, эксплуатацией, включая сопровождение, снятием с эксплуатации объектов информационной инфраструктуры оператора АИС страхования, размещением, хранением и (или) иной обработкой информации, формируемой и (или) получаемой оператором АИС страхования при выполнении своих функций (далее – поставщики услуг в сфере информационных технологий);

требования к тестированию операционной надежности технологических процессов;

требования к нейтрализации информационных угроз со стороны несанкционированного доступа работников оператора АИС страхования или работников поставщиков услуг в сфере информационных технологий, обладающих полномочиями доступа к объектам информационной инфраструктуры (далее – внутренний нарушитель), к объектам информационной инфраструктуры;

требования к обеспечению осведомленности оператора АИС страхования об актуальных информационных угрозах, которые могут привести к инцидентам операционной надежности;

требования к обеспечению защиты критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы работников оператора АИС страхования.

В целях разработки и выполнения требований к операционной надежности, установленных настоящим пунктом, оператор АИС страхования должен определить состав организационных и технических мер, направленных на реализацию усиленного уровня защиты, предусмотренного пунктом 6.8 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.4-2022 «Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 22 декабря 2022 года № 1549-ст «Об утверждении национального стандарта Российской Федерации»[1].

6.1 Оператор АИС страхования должен обеспечивать организацию учета и контроля состава следующих элементов:

технологических процессов, реализуемых непосредственно оператором АИС страхования;

подразделений (работников) оператора АИС страхования, ответственных за разработку технологических процессов, поддержание их выполнения, реализацию технологических процессов (далее – подразделения оператора АИС страхования);

объектов информационной инфраструктуры оператора АИС страхования, задействованных при выполнении каждого технологического процесса;

технологических участков технологических процессов (при наличии);

технологических процессов, технологических участков технологических процессов (при наличии), реализуемых поставщиками услуг в сфере информационных технологий;

работников оператора АИС страхования или иных лиц, осуществляющих физический и (или) логический доступ, или программных сервисов, осуществляющих логический доступ к объектам информационной

[1] М., ФГБУ «Институт стандартизации», 2023.

инфраструктуры (далее – субъекты доступа), задействованных при выполнении каждого технологического процесса;

взаимосвязей и взаимозависимостей оператора АИС страхования со страховщиками, государственными органами, иными лицами, которым государством делегированы властные полномочия, перечень которых установлен Правительством Российской Федерации по согласованию с Банком России в соответствии с пунктом 8 статьи 33.10 Закона Российской Федерации № 4015-I, предоставляющими информацию в АИС страхования, и поставщиками услуг в сфере информационных технологий в рамках выполнения технологических процессов (далее при совместном упоминании – участники технологического процесса);

каналов передачи защищаемой информации, установленной нормативным актом Банка России, принятым на основании подпункта 5 пункта 7 статьи 33.10 Закона Российской Федерации № 4015-I в части установления требований к обеспечению защиты информации, обрабатываемой и передаваемой в рамках технологических процессов участниками технологического процесса.

В целях организации учета и контроля состава технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий, оператор АИС страхования должен обеспечивать ведение отдельного реестра технологических процессов, технологических участков технологических процессов, реализуемых поставщиками услуг в сфере информационных технологий, в соответствии с внутренними документами.

Оператор АИС страхования в отношении элементов, указанных в подпункте 6.1 настоящего пункта, являющихся значимыми объектами критической информационной инфраструктуры в соответствии с пунктом 3 статьи 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ), должен выполнять требования по

обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные в соответствии с пунктом 4 части 3 статьи 6 Федерального закона № 187-ФЗ.

6.2 Оператор АИС страхования должен обеспечивать выполнение следующих требований к управлению изменениями критичной архитектуры:

управление уязвимостями в критичной архитектуре, из-за которых могут реализоваться информационные угрозы и которые могут повлечь превышение значений целевых показателей операционной надежности;

планирование и внедрение изменений в критичной архитектуре, направленных на обеспечение недопустимости невыполнения или ненадлежащего выполнения оператором АИС страхования своих функций;

управление конфигурациями (настраиваемыми параметрами) объектов информационной инфраструктуры;

управление уязвимостями и обновлениями (исправлениями) объектов информационной инфраструктуры.

6.3 Оператор АИС страхования должен обеспечивать выполнение следующих требований к выявлению, регистрации инцидентов операционной надежности и реагированию на них, а также восстановлению выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации таких инцидентов:

выявление и регистрация инцидентов операционной надежности;

реагирование на инциденты операционной надежности в отношении критичной архитектуры;

восстановление функционирования технологических процессов и объектов информационной инфраструктуры после реализации инцидентов операционной надежности;

проведение анализа причин и последствий реализации инцидентов операционной надежности;

организация взаимодействия между подразделениями оператора АИС страхования, а также между оператором АИС страхования и Банком России,

иными участниками технологического процесса в рамках реагирования на инциденты операционной надежности и восстановления выполнения технологических процессов и функционирования объектов информационной инфраструктуры после реализации инцидентов операционной надежности.

6.4 Оператор АИС страхования должен обеспечивать выполнение следующих требований к взаимодействию с поставщиками услуг в сфере информационных технологий:

управление риском реализации информационных угроз при привлечении поставщиков услуг в сфере информационных технологий, в том числе защита своих объектов информационной инфраструктуры от возможной реализации информационных угроз со стороны поставщиков услуг в сфере информационных технологий;

управление риском технологической зависимости функционирования своих объектов информационной инфраструктуры от поставщиков услуг в сфере информационных технологий.

6.5 Оператор АИС страхования в части тестирования операционной надежности технологических процессов должен принимать организационные и технические меры, направленные на проведение сценарного анализа (в части возможной реализации информационных угроз в отношении критичной архитектуры, а также возникновения сбоев объектов информационной инфраструктуры), и проводить с использованием результатов сценарного анализа тестирование готовности оператора АИС страхования противостоять реализации информационных угроз в отношении критичной архитектуры.

6.6 Оператор АИС страхования в части нейтрализации информационных угроз со стороны внутреннего нарушителя разрабатывает и принимает организационные и технические меры в отношении субъектов доступа, привлекаемых в рамках выполнения технологических процессов, направленные на исключение возможности несанкционированного использования предоставленных указанным субъектам доступа полномочий.

6.7 Оператор АИС страхования должен обеспечивать выполнение следующих требований к обеспечению осведомленности об информационных угрозах:

организация взаимодействия оператора АИС страхования и иных участников технологического процесса при обмене информацией об актуальных сценариях реализации информационных угроз;

использование информации об актуальных сценариях реализации информационных угроз в целях обеспечения непрерывного выполнения оператором АИС страхования своих функций.

6.8 Оператор АИС страхования в части обеспечения защиты критичной архитектуры от возможной реализации информационных угроз в условиях дистанционной (удаленной) работы работников оператора АИС страхования разрабатывает и принимает организационные и технические меры, направленные на обеспечение непрерывного выполнения оператором АИС страхования своих функций при выполнении работниками оператора АИС страхования своих трудовых функций дистанционно.

7. Оператор АИС страхования разрабатывает и принимает организационные и технические меры, направленные на нейтрализацию угроз в отношении возникновения зависимости обеспечения операционной надежности от субъектов доступа – работников оператора АИС страхования, обладающих уникальными знаниями, опытом и компетенцией в области разработки технологических процессов, поддержания их выполнения, реализации технологических процессов, которые отсутствуют у иных работников оператора АИС страхования.

8. Оператор АИС страхования должен установить во внутренних документах описание процедур, направленных на реализацию требований к операционной надежности, включая:

определение и описание состава процедур, направленных на выполнение требований к операционной надежности;

определение перечня и порядка организационного взаимодействия

подразделений оператора АИС страхования, участвующих в соблюдении требований к операционной надежности, с учетом исключения конфликта интересов;

определение порядка осуществления контроля за соблюдением требований к операционной надежности в рамках системы внутреннего контроля;

выделение ресурсного обеспечения для выполнения требований к операционной надежности;

порядок утверждения и условия пересмотра процедур, направленных на выполнение требований к операционной надежности;

порядок регистрации инцидентов операционной надежности.

Оператор АИС страхования должен обеспечить реализацию требований к операционной надежности, начиная с разработки и планирования внедрения технологических процессов.

Порядок регистрации инцидентов операционной надежности должен предусматривать регистрацию по каждому инциденту операционной надежности оператором АИС страхования:

данных, используемых для фиксации превышения установленных значений целевых показателей операционной надежности;

данных, позволяющих выявить причину превышения установленных значений целевых показателей операционной надежности;

результата реагирования на инцидент операционной надежности (принятых мерах и проведенных мероприятиях по реагированию на выявленный оператором АИС страхования или Банком России инцидент операционной надежности).

9. В целях реализации требований к операционной надежности оператор АИС страхования должен:

моделировать информационные угрозы в отношении критичной архитектуры;

планировать применение организационных и технических мер,

направленных на реализацию требований к операционной надежности, с учетом результатов идентификации риска информационной безопасности, а также его оценки;

обеспечивать реализацию требований к операционной надежности на стадиях создания, ввода в эксплуатацию, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, вывода из эксплуатации объектов информационной инфраструктуры;

обеспечивать контроль соблюдения требований к операционной надежности.

10. Оператор АИС страхования в рамках обеспечения операционной надежности должен информировать Банк России:

о выявленных инцидентах операционной надежности, включенных в перечень типов инцидентов операционной надежности (в случае превышения допустимой доли деградации технологических процессов), а также о принятых мерах и проведенных мероприятиях по реагированию на выявленный оператором АИС страхования или Банком России инцидент операционной надежности;

о планируемых мероприятиях по раскрытию информации, включая выпуск пресс-релизов и проведение пресс-конференций, размещение информации на своем официальном сайте в сети «Интернет», в отношении указанных в абзаце втором настоящего пункта инцидентов операционной надежности не позднее одного рабочего дня до дня проведения мероприятия.

Оператор АИС страхования должен представлять в Банк России указанные в абзацах втором и третьем настоящего пункта сведения с использованием технической инфраструктуры (автоматизированной системы) Банка России или резервного способа взаимодействия (при технической невозможности использования технической инфраструктуры (автоматизированной системы) Банка России), информация о которых размещается на официальном сайте Банка России в сети «Интернет».

11. Настоящее Положение подлежит официальному опубликованию и

в соответствии с решением Совета директоров Банка России (протокол заседания Совета директоров Банка России от _____ года № ПСД-_____) вступает в силу с 1 апреля 2024 года, за исключением абзаца десятого пункта 6 настоящего положения, который вступает в силу с 1 января 2025 года.

Председатель
Центрального банка
Российской Федерации Э.С. Набиуллина

Приложение
к Положению Банка России
от «__»_____ 202_года №___-П
«О требованиях к операционной надежности, которые обязан соблюдать оператор автоматизированной информационной системы страхования»

Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов оператора АИС страхования

№	Наименование технологического процесса	Пороговый уровень допустимого времени простоя и (или) деградации технологических процессов (в часах)
1	2	3
1	Технологический процесс, обеспечивающий получение и обработку оператором АИС страхования информации, предусмотренной пунктом 1 статьи 33.11 Закона Российской Федерации № 4015-1	24
2	Технологический процесс, обеспечивающий предоставление информации, содержащейся в АИС страхования, пользователям АИС страхования в целях заключения договоров обязательного страхования в виде электронных документов	0,5

1	2	3
3	Технологический процесс, обеспечивающий предоставление информации, содержащейся в АИС страхования, пользователям АИС страхования в целях, предусмотренных Федеральным законом от 25 апреля 2002 года № 40-ФЗ «Об обязательном страховании гражданской ответственности владельцев транспортных средств»[1], за исключением заключения договоров обязательного страхования в виде электронных документов	8
4	Технологический процесс, обеспечивающий работу сайта оператора АИС страхования в информационно-телекоммуникационной сети «Интернет»	8

[1] Собрание законодательства Российской Федерации, 2002, № 18, ст. 1720.