Юрий Ногин
начальник Управления
риск-менеджмента
УК «Ингосстрах – Инвестиции»

Дмитрий Сидоров
руководитель направления
по управлению операционными рисками
УК «Ингосстрах – Инвестиции»

Исключение форс-мажора

Особенности контроля операционной надежности и выполнения новых требований по информационной безопасности в НФО

Вначале обозначим, что следует понимать под термином «операционная надежность».

Под операционной надежностью (в соответствии с Положением Банка Россия от 15.11.2021 г. N779-П «Об установлении обязательных для НФО требований к операционной надежности») понимается способность НФО обеспечить непрерывность функционирования критически важных процессов при осуществлении профессиональной (лицензируемой) деятельности в условиях реализации информационных угроз. Организация непрерывности и восстановления деятельности (далее — ОниВД) в НФО — это стратегия подготовки к различным форс-мажорным ситуациям, влияющим на критичные процессы и технологические участки в НФО. Сейчас такая стратегия актуальна как никогда. Операционная надежность, на наш взгляд, должна выступать одним из ключевых элементов процесса мониторинга нарушений повседневного функционирования организации и иных чрезвычайных ситуаций. Являясь инструментом наблюдения и реагирования на инциденты, связанные с прерыванием ключевых процессов, операционная надежность должна рассматриваться некоммерческой финансовой организацией в рамках

Табл. 1

Мера	Подходы		
	Формальный	Сбалансированный	Заинтересованный
Внедрение со стороны Регулятора[1] требования о наличии в НФО отдельной должности, ответственной за управление операционными рисками, операционной надежностью и непрерывностью деятельности.	Назначение работника, совмещающего основную деятельность с функциями по операционной надежности.	Выделение отдельного работника.	Выделение отдельного подразделении.
Повышение риск-культуры через обязательное проведения как внутренних, так и внешних семинаров и лекций на соответствующие темы.	–	Периодически один-два раза в год.	На ежеквартальной основе.
Тестирование работников и процессов операционной надежности.	–	Периодически один-два раза в год.	На ежеквартальной основе.

[1] Банк России

Табл. 2

Мера	Подходы		
	Формальный	Сбалансированный	Заинтересованный
Вовлеченность персонала	Низкая вовлеченность.		
Обучение проходит один раз в год и реже.	Средняя и высокая вовлеченность.		
Обучения проходят два раза в год и чаще.	Высокая вовлеченность работников.		
Наличие метрик по работе с инцидентами, влияющими на KPI.			
Регулярные семинары.			
Сбор статистики по инцидентам с оценкой возможного ущерба, затрат на минимизацию рисков и обоснованием экономического эффекта, благодаря этой статистике становится понятным, почему имеет смысл выявлять и минимизировать инциденты.	Вынесение отчетов по руководству раз в полгода / год.	Вынесение отчетов по руководству раз в квартал / месяц.	Вынесение отчетов по руководству ежемесячно / еженедельно.
Политика награждения за выявленные инциденты.	–	–	Дополнительное материальное поощрение.

планов и сценариев реагирования по ОНиВД.

На основе практики внедрения операционной надёжности в различных НФО можно выделить три основных подхода к организации процесса.

1. Формальный подход, как, правило, присущ небольшим «молодым» НФО с неразвитой риск-культурой, которые стремятся обеспечить исполнение регуляторных требований в части операционной надежности минимальными вложениями ресурсов. Данные подход характеризуется наличием «ручных» контролей, минимальным числом персонала, отсутствием автоматизации бизнес-процесса.
2. Сбалансированный подход, в соответствии с принципом экономической целесообразности, присущ всем НФО с развитой риск-культурой. Характеризуется взвешенными решениями в части внедрения автоматизации бизнес-процесса операционной надежности, наличием профильных специалистов, внедрением как «ручных», так и автоматизированных контролей.
3. Заинтересованный подход присущ организациям с продвинутой риск-культурой. Как правило, это крупные «опытные» НФО, ответственно относящиеся к непрерывности деятельности своих продуктов, сервисов и приложений. Характеризуются тем, что в рамках организации и поддержания процесса операционной надежности выделяют на это отдельных экспертов и (или) подразделения, выделяют также финансирование, имеют автоматизированные контроли, постоянную отчетность для руководства, взаимодействуют с Банком России, внедряют новые практики.

К особенностям контроля за операционной надежностью можно отнести проблемы, возникающие при исполнении Положения Банка России от 15.11.2021 г. №779-П, разделив их на организационные и технические.

Организационные проблемы

1. Отсутствие у работников НФО понимания проблематики операционной надежности. В ряде российских НФО недостаточно развита риск-культура и отсутствует опыт работы с инцидентами операционной надежности. В связи с этим далеко не все работники и руководители осознают потенциальные угрозы, связанные с недостаточным контролем операционной надежности. Регуляторные требования соблюдаются по остаточному признаку и не учитываются в операционной деятельности организации.

Возможное решение проблемы изложено в таблице 1.

Следует заметить, что НФО ожидают получить от Регулятора требования к работникам, обеспечивающим операционную надежность, в части квалификации и минимальных знаний, обучения и аттестации работников НФО с необходимым уведомлением Регулятора, а также для получения соответствующих сертификатов.

2. Сокрытие информации со стороны работников НФО. Желание утаить, «спрятать» проблему является естественной реакцией человека на угрозу. Оно связано, во-первых, с недостаточным пониманием того, что надо делать в сложившейся ситуации, во-вторых, с потенциальными негативными последствиями для работника, выявившего инцидент. Подходы к комплексному решению проблемы изложено в таблице 2.

Кроме того, необходим ряд дополнительных мер. В их числе: 1) сбор статистики по инцидентам с оценкой возможного ущерба, затрат на минимизацию рисков и обоснованием экономического эффекта. Благодаря такой статистике становится понятным, почему имеет смысл выявлять и минимизировать инциденты; 2) внедрение метрик эффективности работы с операционными рисками, инцидентами операционной надежности и мерами минимизации рисков для подразделений, поощрение (финансовая мотивация) работников за счет сэкономленных средств; 3) доведение до сведения работников НФО информации о недопустимости «наказания» за выявление потенциальных угроз и нулевая толерантность к случаям внутреннего мошенничества; 4) доведение информации об результатах применения мер по митигации рисков до руководства.

3. Сокрытие информации непосредственно самой НФО (репутационные риски организаций). Причиной является незаинтересованность НФО открыто говорить о проблемах внутреннего характера, приводящих к нарушениям операционной надежности по вине работников организации, в случаях халатности, ненадлежащего внутреннего контроля и различного рода форс-мажорных обстоятельств. Любая организация не заинтересована распространять информацию о внутренних проблемах, существенно влияющих на клиентский сервис, так как это приводит к увеличению репутационных рисков и, как следствие оттоку клиентов, недоверию широких масс населения. Особенно это актуально для крупных брендов и групп компаний.

В этом случае могут быть два решения. Во-первых, можно пойти по пути неотвратимости и ужесточения наказания Банка России за сокрытие информации НФО, выявленных при проверках (что будет стимулировать к переходу от формального подхода к более продвинутым «жестким сценариям». Во-вторых,

можно создать мотивационную систему, например, снижающую нагрузку на капитал для НФО, своевременно и полноценно контролирующих инциденты операционной надежности. Это «мягкий сценарий».

Некачественное (недостаточное) управление рисками информационной безопасности (далее — ИБ). Инциденты операционной надежности представляют собой частные случаи рисков ИБ. При разработке мер минимизации требуется обязательное участие представителей подразделения, ответственных за обеспечение в организации ИБ информационных технологий, а также подразделений-владельцев процесса.

Необходима регламентация сроков проведения расследований и принятия решений, что способствует своевременному реагированию на инциденты. В части их предотвращения целесообразно использовать опыт других организаций, проводя сценарный анализ известных случаев (из открытых источников).

Технические проблемы

4. Сложность трансформации данных из учетных систем НФО в формат отчетности Банка России. Различные учетные системы по-разному выгружают данные, что серьезно увеличивает время подготовки регуляторной отчетности.

Решение: разработка и описание конверторов из наиболее популярных учетных систем, а также взаимодействие с техническими специалистами Регулятора.

5. Недостаток опыта информирования АСОИ ФинЦерт: отсутствие у подразделений/ответственных работников, занимающихся мониторингом инцидентов операционной надежности в НФО, реальной практики работы с программным обеспечением «Континент TLS-клиент» для передачи информации в подразделении ИБ Банка России. Решением данной проблемы являться обучение использованию соответствующего программного обеспечения со стороны представителей ИБ Банка России.

6. Отсутствие полноценного мониторинга всех процессов НФО, связанных с инцидентами операционной надежности, в том числе ИТ-систем и ключевых процессов. Зачастую для некрупных НФО внедрение мониторинга производительности ИТ-систем связано с экономической нецелесообразностью, наряду с этим не каждая ИТ-система имеет развитое логирования всех действий, что необходимо для контрольной функции. Это, зачастую, приводит к длительному проведению расследований по инцидентам (увеличивается время между выявлением и принятиям соответствующих мер по минимизации).

Решением проблемы является:

- проведение IT-аудита информационных систем в части мониторинга и логирования, принятия решения о необходимости внедрения автоматизированного мониторинга за ключевыми системами и процессами в НФО;
- поиск и применение готовых промышленных решений с расширенным функционалом;
- взаимодействие с вендорами программного обеспечения по внесению доработок и настройки ПО для нужд конкретной НФО.

7. Отсутствие промышленных программных решений и стандартов в части контроля операционной надежности. На сегодняшний день у НФО нет 100% уверенности в том, что все инциденты операционной надежности выявляются и фиксируются,поскольку нет единого стандарта их контроля.

Здесь решение по объективным причинам не может быть найдено в ближайшее время, так как отсутствует наработанная статистика удачных «правильных» разрешений проблем. Исторически рынок всегда смотрит на позицию Регулятора, ожидая разъяснений и описанных стандартов, по которым могут быть разработаны промышленные программные продукты. ◻