Через призму рисков и инцидентов

Процесс перехода на риск-ориентированный подход управления киберрисками и операционной надежностью подходит к тому этапу, когда можно будет делать первые выводы. Но понятно одно: малым и средним компаниям будет сложно

Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**



Управление операционной надежностью и рисками информационных угроз является сложным и длительным процессом, требующим непрерывного внимания и управления этапами процесса внедрения. Тем не менее грамотная организация процесса может значительно повысить эффективность защиты информационных систем и снизить возможность возникновения проблем и угроз.

В широком понимании операционная надежность — это способность информационных систем функционировать без инцидентов и сбоев, обеспечивать высокую доступность и непрерывность предоставления сервисов. Операционная надежность напрямую связана с управлением рисками и предотвращением угроз IT и ИБ, которые могут привести к нарушению работы системы, утечке или повреждению информации.

Отчетность все покажет

Банк России применительно к специфике финансового сектора предлагает четкую регуляторную установку: «Финансовые организации должны обеспечить операционную надежность в условиях реализации информационных угроз». Такая формулировка снимает с повестки дискуссию о необязательности этой процедуры.

О деталях того, что регулятор имеет в виду, в ходе сессии «Финансовая отрасль: операционная надежность и киберриски» в рамках Второй межотраслевой конференции по регуляторике в сфере ИБ, организованной АБИСС (Ассоциацией пользователей стандартов по информационной безопасности), говорилось в докладе **Антона Чернодеда,** начальника отдела методологии контроля и наблюдения департамента информационной безопасности Банка России. По словам эксперта, регулятор рассматривает три основных сценария реализации атак, в результате которых возможны максимально негативные потери. Это, во-первых, атаки на системы, которые входят в контур системы управления операционным риском. На верхних строках списка угроз

находятся DDoS-атаки и отзыв сертификатов безопасности (TLS). Затем располагаются угрозы со стороны вредоносного ПО, включая шифровальщики типа WannaCry, а также риски, генерируемые наличием иностранного оборудования и ПО. Во-вторых, атаки на участок взаимодействия с платежной системой Банка России. В-третьих, социальная инженерия в отношении клиентов кредитных организаций.

Что касается управления операционным риском, то выстраивается система, в которую в том числе входят оценка качества выполнения процедур на базе Положения Банка России № 716-П, а также оценки нарушения нормативов Н1.0, Н1.1 и Н1.2 в стрессовом сценарии [(ВПДОК (внутренние процедуры оценки достаточности капитала), нормативный акт Банка России «Об оценке качества внутренних процедур оценки достаточности капитала»].

Антон Чернодед упомянул о том, что в 2022 году вступили в силу два положения Банка России, касающиеся операционной надежности для КО и НКО, в которых определен перечень контролируемых технологических процессов: 60 и 13 штук соответственно. Сейчас, год спустя, регулятор начал выстраивать работу по пересмотру этих списков, что происходит в соответствующей рабочей группе при Банке России. К работе в ней приглашаются все заинтересованные организации.

Кроме того, уже один раз кредитные организации сдали шесть форм отчетности, касающиеся обеспечения операционной надежности. В апреле 2023 года ожидается вторая волна сдачи, которая должна обобщить информацию о соответствующих показателях, дополненных информацией об IT-инфраструктуре финансовых организаций. К этому времени планируется выпуск методических рекомендаций в части уточнения наименования объектов инфраструктуры, учитываемых в формах отчетности.

«Всё, дальше сами!»

«А есть ли уже опыт подсчета эффективности внедренных требований, реализованных новых или измененных существующих процессов в контексте перехода к риск-ориентированному подходу?» — задала участникам круглого стола непростой вопрос **Анастасия Харыбина,** председатель АБИСС,.

Юлия Литикова, руководитель направления IT-аудита банка «Тинькофф», высказала такое мнение: «Прошло еще очень мало времени со старта. Что касается процессов, то они выстраиваются, меняются, комбинируются и т.д. Но накопленный опыт позволяет говорить о том, что это не какие-то совсем новые процессы, ведь и до этого осуществлялся мониторинг наиболее критичных из них».

В итоге может сложиться неверное впечатление о том, что стоимость осуществляемой трансформации весьма высока, а достигнутая эффективность сомнительна.

Артем Калашников, управляющий директор Центра информационной безопасности дочерних и зависимых обществ Газпромбанка, был категоричен в этом вопросе: «Топ-менеджмент банков весьма заинтересован в успехе реализуемых начинаний. Ведь если менеджмент хочет чем-то управлять, он должен понимать, что в этих всех рисках заложено на самом деле. И их оценка происходит через осознание руководством суммы ущерба от инцидентов ИБ, а ориентировочные потери по итогам событий 2022 года понятны, велики и идентифицируемы. Например, выключенное по каким-либо причинам средство безопасности сегодня приведет к тому, что с вероятностью 99% бизнес работать перестанет. Таким образом, что касается IT и ИБ — эффект уже есть, рисковики догонят».

Александр Кондратенко, начальник управления рисками и развитием процессов информационной безопасности Росбанка, согласен: «Действительно, оценивать необходимо через призму рисков и инцидентов, как внутренних, так и внешних. А тот факт, что у нас не происходит того, что погубило кого-то другого, и есть доказательство эффективности».

С чего начинался процесс выстраивания управления операционной надежностью и рисками информационных угроз в этих банках? Во-первых, департаменты рисков, IT и ИБ учились работать сообща. Довольно неожиданным первым эффектом стало понимание того, что процессы, протекающие в этих структурных подразделениях, имеют множество пересечений, а риски, изначально классифицированные как, например, ИБ, через час могут быть переведены в IT-риски. Поэтому задача скорее состояла в модификации и классификации процессов для увязки их с нормативными документами и формирования обязательной отчетности.

С точки зрения развертывания систем GRC (Governance, Risk and Compliance) все крупные банки выбрали путь собственной разработки. С одной стороны, в этом есть определенный резон — не бывает двух одинаковых крупных финансовых структур с их уникальным аппетитом к риску, а также, как привыкли выражаться западные бизнес-консультанты, с персональным Risk Awareness (осведомленностью о рисках).

Почему это так важно? Риск-ориентированный подход невозможно внедрить без самого активного участия в этом топ-менеджмента, которое зачастую выражается в персональном погружении в суть подхода, а также в выстраивании собственных бизнес-коммуникаций с соответствующими департаментами, от которых ранее чаще всего требовалось наличие в рабочем кабинете сертификата о соответствии «бумажной безопасности» в красивой рамке.

На практике эти коммуникации обычно проявляются в совместном с департаментами рисков, ИБ и IT выстраивании адекватных внешней обстановке и собственным бизнес-задачам риск-моделей, которые отражают внутреннее видение того, какая информация важна, на что необходимы инвестиции в первую очередь, какие риски можно принять или застраховать.

Все сказанное, как выразился Артем Калашников, означает только одно: «На рынке вряд ли когда-либо появится промышленная GRC-система "из коробки", сразу готовая к работе. Возможно, благодаря достижениям лидеров выйдет урезанная, усеченная версия с минимальным набором модулей, позволяющих выполнить некоторые обязательные регуляторные функции. Наполнение остальных модулей обеспечивает конкурентное преимущество банков-первопроходцев. Мы, возможно, с коллегами примем участие в появлении такой light-системы. Всё, дальше сами!». Б.О