Риск начальника боится

Почему не обойтись без топ-менеджмента при управлении рисками информационных угроз и обеспечении операционной надежности

Текст
АЛЕКСАНДР МОИСЕЕВ,
ВЕДУЩИЙ КОНСУЛЬТАНТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ AKTIV.CONSULTING

С 1 февраля 2023 года введены в действие два новых стандарта ГОСТ Р 57580.3-2022 и ГОСТ Р 57580.4-2022, которые детализируют ряд требований к основным процессам управления риском реализации информационных угроз (УР ИУ) и обеспечения операционной надежности (ОН) финансовых организаций, закрепленных в положениях Банка России, в виде базового состава мер в табличной форме.

Рассмотрим ключевую проблему — вовлечение руководства финансовых организаций в процессы УР ИУ и обеспечения ОН, ведь их участие устанавливается в положениях Банка России, Указе Президента Российской Федерации от 1 мая 2022 года № 250 (детализируется в Постановлении Правительства РФ от 15 июля 2022 года № 1272), а также закреплено в ряде мер новых стандартов:

- для ГОСТ Р 57580.3 — ОПР.7,8.5,18-20; ЗИУ.10-11; УПК.7,12,16; ОС3.3.4-3.5;
- для ГОСТ Р 57580.4 — ВРВ.41-42.

Очевидно, что, согласно концепции регулятора, топ-менеджмент должен выступать внутренним заказчиком для внедрения процессов УР ИУ и ОН в финансовых организациях (ФО) для обеспечения их устойчивости. Но на деле зачастую данные процессы отдаются в лучшем случае на откуп линейным подразделениям ИБ, IT и службы управления рисками, а в худшем — замыкаются только на ИБ.

Основные причины сложившейся ситуации

1. Низкий приоритет вопросов ИБ/IT по сравнению с вопросами операционной деятельности. Традиционно для руководства ФО на первом месте стоят понятные и привычные для них процессы, связанные с процессингом, клирингом, работой с клиентами.

2. Сложность коммуникации между ИБ и бизнесом. В большинстве органи-

заций они находятся в разных плоскостях: службы ИБ смотрят в функциональной плоскости — риски, требования регулятора, новые уязвимости, новые техники и тактики проникновения в IT-инфраструктуру и т.п., а бизнес мыслит процессами, такими категориями, как «совокупная стоимость владения», «окупаемость инвестиций», «амортизация», «стоимость обучения персонала» и «организация технической поддержки» и т.д.

3. Низкая осведомленность об актуальных информационных угрозах. Вследствие бурного развития IT-технологий, даже имея профильное образование или пройдя профессиональную переподготовку, необходимо постоянно держать руку на пульсе, чтобы понимать последствия реализации тех или иных угроз для бизнеса и заблаговременно принимать меры.
4. Восприятие требований регулятора как «очередной комплаенс». К сожалению, в отношении комплаенса исторически сложилось мнение, что достаточно разработать комплект определенных регламентов, а фактически их исполнять необязательно.

Хотя бы одна из названных причин (если не все) актуальна для многих организаций. Чем грозит бездействие в решении проблемы невовлеченности руководства? Прежде всего возникновением реальных финансовых и репутационных потерь в случае реализации инцидента защиты информации или ОН. Причем пострадать могут партнеры и клиенты не только самой финансовой организации, но и «цепочки поставок» или экосистемы финансовых продуктов.

Как можно улучшить ситуацию?

Нужен импульс изнутри, и по сложившейся практике он должен исходить именно от службы ИБ. Что может помочь?

1. Формирование картины целевого состояния процессов УР ИУ и ОН — «как должно быть». Необходимо в течение имеющегося срока адаптации к требованиям новых стандартов в инициативном порядке выйти на диалог с бизнесом, сформировать верхнеуровневое видение целевого состояния процессов, то есть определить, к чему мы должны прийти, какие силы и средства задействовать.
2. Обоснование на понятном бизнесу языке. Использовать для этого можно максимально знакомые менеджменту инструменты и привычные форматы подачи информации (BIA, ТЭО, ROI). В своем роде это «инвестиционный проект» по внедрению новых процессов, а значит, нужен «бизнес-план», который опишет, сколько это будет стоить и какую ценность привнесет.
3. Повышение осведомленности руководства в части ИБ. Помимо общих программ повышения осведомленности для всех сотрудников ФО для назначенных ответственных кураторов по направлению ИБ на периодической основе необходимо проводить обучение.
4. Планировать и внедрять изменения в существующие бизнес-процессы необходимо с помощью проектного подхода, что позволит не только донести суть изменений до руководства и контролировать ресурсы, но и всем участвующим подразделениям согласовать распределение ролей и обязанностей.

Рассмотрим примеры процессов, в которых, согласно новым стандартам, требуется участие топ-менеджмента.

В таблице выделяется несколько условных уровней взаимодействия: стратегический — в перспективе трех — пяти лет и более, тактический — в пределах планового периода в один год, операционный — ежедневно в течение текущего года.

В левом столбце таблицы для каждого из уровней приведено по два примера процессов, в которых требуется обязательное участие топ-менеджмента. В правом столбце даны рекомендации, которые, по опыту, способствуют решению задачи вовлечения руководства в процессы УР ИУ и ОН.

Начнем с обязательных требований.

На стратегическом уровне — это учет рисков ИУ при разработке стратегии финансовой организации, а также при рассмотрении крупных инвестиционных проектов. Помимо этого к обязательным требованиям относится утверждение политики по управлению рисками реализации информационных угроз, распределяющих роли и обязанности в рамках концепции «трех линий защиты», описанных в ГОСТ.

ТРЕБУЕМЫЕ ПРОЦЕССЫ	РЕКОМЕНДУЕМЫЕ ПРОЦЕССЫ
Стратегический уровень	
Учет рисков информационных угроз в рамках общей стратегии ФО	Включение ИБ в цикл стратегического планирования ФО
Утверждение политики управления риском	
Тактический уровень	
Рассмотрение отчетности по управлению рисками	Повышение осведомленности об ИУ
Утверждение контрольных показателей уровня риска	
Операционный уровень	
Контроль процедур реагирования и восстановления	Обеспечение ситуационного информирования
Контроль результатов аудитов	

На тактическом уровне — это прежде всего хорошо регламентированные и описанные процессы по утверждению контрольных показателей уровня риска, в том числе связанных с оценкой соответствия требованиям положений Банка России, их контрольных и сигнальных значений на плановый годовой период, а также рассмотрение отчетности по управлению рисками, подготовленной в рамках положений ЦБ.

На операционном уровне — это контроль хода реагирования на значительные инциденты или инциденты, связанные с ОН (в том числе компьютерные атаки), и контроль хода восстановительных работ. Контролю подлежат также результаты независимых внутренних и внешних аудитов ФО.

Перейдем к рекомендациям

На стратегическом уровне мы рекомендуем включить ИБ в цикл стратегического планирования, производить экспресс-оценку драфта стратегии на явные стоп-факторы, затем готовить реестр рисков, разрабатывать несколько конфигураций мер митигации (компенсирующих мер), оформлять подраздел по ИБ и уже на этапе реализации стратегии разрабатывать дорожную карту внедрения мер ИБ. Далее следует ее реализация, затем проводится плановый контроль, оформляется отчетность, а в случае изменения условий допускается внеплановый пересмотр стратегии. В результате получаем исправление ошибок на самых ранних этапах разработки стратегии, когда стоимость исправлений минимальна.

На тактическом уровне необходимо повышение осведомленности: разработка программ обучения для ключевых специалистов ФО и кураторов по направлению ИБ, отработка навыков и проверка знаний инженерно-технического персонала по проведению восстановительных работ, планирование и проведение киберучений. В результате получаем поддержание в высокой готовности навыков взаимодействия в кризисной ситуации.

На операционном уровне рекомендуем обеспечение ситуационного информирования куратора по направлению ИБ: оперативное оповещение об инцидентах и угрозах, подготовка ежемесячной сводной аналитики по трендам отраслевых инцидентов на основе реальных данных (по каналам ФинЦЕРТ/TI), информирование о значимых инцидентах у клиентов и партнеров из смежных отраслей. В результате получаем постепенное включение вопросов ИБ и ОН в повестку ответственного куратора наравне с операционной деятельностью.

В качестве резюме

Проблема недостаточного вовлечения топ-менеджмента в процессы решаема, но отказ от систематической работы с ней, обосновывая и разъясняя важность участия, не приведет к изменению ситуации. Лидерство в данном вопросе оптимально возложить на службу ИБ, но при этом подчеркивать, что итоговые решения по УР ИУ и по обеспечению ОН — задача менеджмента. Подводя итог всему сказанному, подчеркну, что комплаенс сегодня — это не только работа с документами, но и организация реально функционирующих процессов. **Б.О**