АССОЦИАЦИЯ
безопасности бизнеса и комплаенса
сообщество экспертов бизнес-этики и управления рисками

«РЕЙД-НА-РАССВЕТЕ»: ПРОТОКОЛ САМОЗАЩИТЫ

практики антикризисного управления, непрерывности деятельности компании и устойчивости бизнеса в случае «визита» правоохранительных органов / «когда вами заинтересовались»

практические рекомендации от Ассоциации безопасности бизнеса и комплаенса

версия 2022

«Визит» правоохранительных органов – это не просто стресс. Это **серьезная турбулентность для бизнеса и безусловная кризисная ситуация**. В рамках нашего телеграм-канала «Клуб корпоративной безопасности» мы провели опрос. Треть участников заявили, что их компания в значительной мере уделяет внимание разработке антикризисных мер (на случай «визита») и верит в их эффективность. В тоже время 40% отметили, что им крайне необходимы целостная система антикризисного управления, отмечая высокую степень опасения столкнуться с «коллапсом» бизнеса. Любопытно то, что оставшиеся 30% выразили сомнение в том, что можно оказать влияние на развитие событий, если бизнесом уже «заинтересовались» соответствующие инстанции. Это может говорить о том, что и такая часть компаний «слабо» готова к таким кризисным ситуациям.

Подобные результаты подтверждаются нашими интервью с адвокатами, которые отмечают, что **в подавляющем большинстве случаев бизнес, его собственники и руководители не готовы к таким кризисам**. Более того, мы опросили собственников и руководителей, кто лично прошел через такой «опыт». Почти все, оглядываясь назад, однозначно утверждают, что предварительная подготовка к такому развитию событий, оказала бы серьезную поддержку их бизнесу как во время самого «рейда-на-рассвете», так и во время сложного периода следственных действий. При этом существенная часть опрошенных заявили, что в таких обстоятельствах бизнесы или прекращали свое действие или их размер сокращался минимум в два раза только в течение первого года!

Более того, **ключевой проблемой, с которой сталкиваются адвокаты, защищая руководство и собственников, является т.н. «информационный голод»**. В значительном количестве случаев во время процессуальных действий правоохранительные органы изымают документы, блокируется доступ к ERP и другим информационным системам компании. Если руководство и собственники задержаны – полноценно работать в такой ситуации крайне затруднительно. Адвокат фактически ничего не знает о ключевых аспектах деятельности компании, и крайне слабо представляет с какой «фактурой» он имеет дело. В такой ситуации следствие получает огромное преимущество.

Мы выделили **7 КЛЮЧЕВЫХ УГРОЗ УСТОЙЧИВОСТИ БИЗНЕСА** для такой кризисной ситуации:

1) **Потеря** существенного контроля над компанией / бизнесом;
2) **Безопасность** «ключевых» лиц (собственники, руководители и топ-менеджеры);
3) **Угроза** стратегической устойчивости, т.е. при которой компания испытывает давление по стратегическим направлениям: ключевые клиенты, источники финансирования и т.п.
4) **Доступность** информации (информационных систем) и документов;
5) **Технические препятствия** для операционного управления (широкий спектр);
6) **Угрозы** невыполнения обязательств (как компанией, так и ее контрагентами);
7) **Репутационный ущерб**.

Вот почему мы рекомендуем должным образом подготовиться. Важность планирования и моделирования таких мероприятий обусловлена и тем, что **в момент активации риска у компании обычно нет достаточно навыков, времени и ресурсов, чтоб адекватно реагировать**.

Опираясь на наш опыт и экспертизу, предлагаем вашему вниманию 20 антикризисных мероприятий, которые мы объединили в две большие группы:

стратегические – мероприятия, которые предоставляют комплексное решение, охватывающее несколько ключевых рисков или имеют «стратегическое» значение для устойчивости бизнеса;

тактические – мероприятия, основная цель которых сосредоточена на одном ключевом риске, даже если достигается позитивный эффект для широкого числа аспектов деятельности компании.

Кроме этого, мы посчитали нужным предложить вам **5 профилактических операционных стримов** деятельности вашей компании, на которые стоит обратить внимание.

С уважением,

Михаил Викторович Черников, Ассоциация безопасности бизнеса и комплаенса, abcom.pro
Адвокат Татьяна Анатольевна Тарахович, lexpro.by

ПРОТОКОЛ: «РЕЙД-НА-РАССВЕТЕ»

рекомендуемые антикризисные мероприятия по обеспечению непрерывности деятельности бизнеса и устойчивости компании в случае «визита» в компанию правоохранительных органов

практические рекомендации от Ассоциации безопасности бизнеса и комплаенса

7 СТРАТЕГИЧЕСКИХ МЕРОПРИЯТИЙ

1. Антикризисная политика. Рекомендуется разработать антикризисную политику, где предусмотреть основные / ключевые риски, которые способны повлиять на фундаментальную устойчивость компании, а также описать основные модели поведения. Кроме этого, рекомендуется разработать подробные протоколы для таких ключевых рисков (обратите внимание на п. 15 и 16).

Рекомендуемые элементы антикризисной политики:

- команда антикризисного управления;
- регламент работы и информационное взаимодействие;
- особые правила контроля за деятельностью компании во время кризиса;
- порядок сопровождения «визита» с распределением ролей и обязанностей.

Очевидно, что антикризисная политика и протокол должны учитывать практики / принципы управления непрерывностью деятельности.

2. Адвокатская защита. Крайне важно заранее разработать модель адвокатской защиты как собственников, так и ключевых лиц. Как правило, целесообразно сформировать «адвокатский пул» с присвоением «координирующей» роли одному из адвокатов. Не стоит рассчитывать, что один адвокат может быть «зарезервирован» для всех. Это одна из типичных ошибок. Кроме этого, помните, что доверенный корпоративный in-house юрист не обладает «адвокатским иммунитетом» и не защищен от раскрытия «узких» мест в случае «запроса» правоохранительных органов.

3. Управление полномочиями и матрица доверенностей. Рекомендуется разработать модель дистрибуции полномочий, чтоб избежать «управленческого паралича» в случае, если собственники и руководители будут ограничены в своих действиях (арест, удаленное управление и т.п.). Не стоит забывать о правилах активации таких полномочий, а также обеспечить формальное соответствие системы менеджмента (приказы, должностные инструкции и т.п.). Кроме этого, рекомендуется оценить необходимость модернизации органов управления (совет директоров, внешнее управление и т.п.), которые могли бы усилить взаимозаменяемость, контроль и управление. Продумайте правило «двух рук» («двух ключей»), внесите соответствующие изменения в учредительные документы.

4. Денежные потоки. Смоделируйте резервные способы управления денежными потоками, которые позволили бы управлять поступлением выручки и совершать платежи. Такими способами могут быть модели уступки требований и передачи долгов, выбор доверенных агентов и счетов для управления денежными потоками, резервные источники финансирования текущих операций или распределение имущества и активов.

5. Резервное копирование. Обеспечьте и контролируйте резервное копирование информационных систем, которые использует компания (комбинируя облачные решения и размещения на физических носителях): от систем управленческого учета до CRM и сайтов. Позаботьтесь о правилах активации доступа доверенных лиц к указанным резервным копиям в случае реализации риска (это могут быть, например, адвокаты или члены совета директоров).

6. Антикризисные коммуникации. Во время кризисных ситуаций часто нет времени на разработку адекватной коммуникационной стратегии. Вот почему стоит заранее сформулировать основные правила и шаблоны. Причем они могут быть как общего плана (например, для работников и СМИ), так и специальные: для поставщиков, клиентов, в рамках конкретного договора или проекта (в т.ч. в рамках мероприятий п. 17 и п. 18.).

7. Обучение и тестирование. Следует разработать программу обучения и обучить сотрудников правилам поведения не только во время «визита» правоохранительных органов (см. п. 13-16), но и проинструктировать о правилах операционной работы в кризисных условиях, уведомить о разработанных антикризисных мерах. Кроме этого, крайне рекомендуется провести тесты, во время которых будет возможность в т.ч. выявить узкие места разработанных антикризисных мероприятий.

13 ТАКТИЧЕСКИХ МЕРОПРИЯТИЙ

8. Поручения. Сформируйте поручения (в широком смысле), которые должны быть исполнены в случае реализации риска. Такие поручения могут быть созданы как собственниками и руководителями для своих адвокатов (ряд адвокатов предлагают такие решения), так и в рамках отдельных задач или структур компании.

9. Цифровая подпись. Убедитесь, что цифровая подпись в компании есть больше, чем у одного сотрудника. Сверьтесь с вашим решением в рамках управления полномочиями и матрицы доверенностей (см. п. 3).

10. Вторая подпись: банк и счет. Убедитесь, что распоряжение счетом может осуществляться больше чем одним сотрудником. Сверьтесь с вашим решением в рамках управления полномочиями и матрицы доверенностей (см. п. 3).

11. Дубликат печати. В ряде случаев печать все еще необходима для определенных документов и действий. Возможно, следует сделать дубликат печати или печати под конкретные документы.

12. Копии документов. Рекомендуется оцифровать (если это не было сделано) и сделать копии (вплоть до нотариальных) важнейших документов компании (устав, договора, доверенности и т.п.). Определитесь с доверенным лицом и местом хранения этих копий. Сверьтесь с мероприятием п. 5 «резервное копирование»). Определитесь с правилами доступа третьих лиц к таким документам.

13. Таблица контактов. Сформируйте список лиц (и их контактных данных), с которыми стоит связаться в случае реализации риска. Убедитесь, что такой список всегда в актуальном состоянии, разослан выбранным лицам как в электронной форме, так и на бумажном носителе (в нескольких копиях). Такой список обязательно должен храниться также у секретаря и на пункте охраны (если есть).

14. Система оповещения. Разработайте правила оповещения сотрудников о наступлении кризисного события, определите формат и контент сообщения и обеспечьте соответствующую инфраструктуру (кто, как и т.п.). Это может быть e-mail рассылка, сообщение в общий чат, sms-оповещение. Рекомендуется включить в шаблон рассылки важную информацию для сотрудников (напомнить о правах, контактах адвокатов, рекомендации воздержаться от определенных противозаконных действий и т.п.).

15. Регламент действий (протокол) «входной группы». Разработайте правила поведения для сотрудников «входной группы» (как правило это ресепшен, секретари и охрана). Включите в регламент рекомендации п. 13 «таблица контактов» и п. 14 «система оповещения». Убедитесь, что в регламент включены правила вызова адвокатов, уведомления руководства. Следует описать права и обязанности «гостей» в том числе в зависимости от ведомственной подчиненности, правила предъявления соответствующих документов и т.п. Допустимо включить в протокол отдельные поручения (см. п.8 «поручения»). Проведите обязательно обучение и тесты (см. п. 6 «обучение и тестирование»).

16. Регламент действий (протокол) работников. Разработайте отдельные правила поведения и важную информацию для всех работников. Определите порядок первичных действий, уделите внимание правилам «подмены» если по тем или иным причинам некоторые коллеги не смогут выполнять свои обязанности. Убедитесь, что работники знают свои права, знают как получить необходимую юридическую помощь, от каких мероприятий стоит воздерживаться или знают какие действия запрещены или противозаконны. Проведите обязательно обучение и тесты (см. п. 6 «обучение и тестирование»).

17. Ключевые клиенты. Отработайте сценарии поведения с ключевыми клиентами и спланируйте резервные действия на случай каких-либо препятствий. Проведите ревизию условий о гарантиях, вашей ответственности в случае нарушения обязательств, а также проработайте альтернативные способы расчетов, включая получение оплат на третьих лиц т.п.

18. Ключевые поставщики. Аспектами, на которых стоит сосредоточиться, могут быть: способы расчетов, прием и хранение грузов, условия переадресации и т.п.

19. Провайдеры и инфраструктура. Предусмотрите альтернативные способы получения услуг и элементов инфраструктуры, которые играют ключевую роль в бизнесе (склад, поставщики специального программного обеспечения и т.п.).

20. Работники. Определите перечень ключевых работников (если у вас до сих пор нет этого списка), оцените риски их «исхода» из компании, отработайте сценарий «массового увольнения», разработайте сценарии аутстафинга и аутсорсинга (в т.ч. смоделируйте бюджет) для временного и оперативного замещения «выбывших» работников.

5 ПРОФИЛАКТИЧЕСКИХ СТРИМОВ ОПЕРАЦИОННОЙ ДЕЯТЕЛЬНОСТИ

1. Соблюдение законодательства и комплаенс. В настоящее время мы можем заявить, что «визит» правоохранительных органов чаще всего имеет под собой «разумные» основания подозревать нарушения действующего законодательства (не стоит думать, что в момент «визита» в офис правоохранительные органы только начинают заниматься делом компании и собирать информацию). Кроме этого, не провоцируйте правоохранительную систему «небрежным» подходом к своим делам. Даже при отсутствии умысла на правонарушение все еще много компаний ведут свои дела и документы так, что у контролирующих и правоохранительных органов есть разумные основания сомневаться в «чистоте» бизнеса. Шаблонные акты или скачанные из интернета договора могут стать триггером. Обеспечьте максимально возможный уровень комплаенса / соответствия требованиям законодательства, проводите регулярные аудиторские проверки и due diligence.

2. Корпоративный климат и лояльность персонала. Во-первых, в ряде случае «рейды-на-рассвете» происходят «благодаря» оперативной информации, полученной сотрудниками правоохранительных органов от самих работников компании. И государство все больше и больше поощряет такую практику (и такой подход не является уникальным и соответствует тренду развитых юрисдикций). Во-вторых, во время оперативных мероприятий нелояльный персонал может проявить себя не лучшим образом. В некоторых ситуациях есть риск прямых оговоров и вранья с целью причинить максимальный ущерб компании или конкретным лицам. Придерживайтесь справедливого подхода к работникам, проявляйте заботу и развивайте корпоративную культуру.

3. Режим конфиденциальности и защита информации. Применяйте хотя бы минимальные «гигиенические и разумные» подходы к защите вашей информации, особенно той, которая в отрыве от контекста может спровоцировать контролирующие или правоохранительные органы. Обязательно разработайте матрицу прав доступа как к конкретным документам, так и к отдельным модулям ваших информационных систем. Кроме этого, рекомендуем (если это возможно) исключить хранение всех электронных документов и информации на локальных дисках компьютеров, следует все максимально перевести в «облака» / на сервера. Внедряйте правила «чистых столов» и «чистых экранов». Отработайте альтернативные способы связи и обмена информацией.

4. Синхронизация управленческого и бухгалтерского учета. Безусловно, само по себе наличие отдельного «управленческого учета» не является чем-то «криминальным». Между тем, помните, что существенные расхождения с «официальной бухгалтерией» является достаточным и разумным основанием для правоохранительных органов, чтобы заподозрить неладное. Кроме этого, обеспечьте отдельное надежное хранение подобных данных, в том числе с учетом рекомендаций в п. 3 в части разграничения прав доступа.

5. Соблюдение принятых обязательств. Недовольные контрагенты могут стать источником информации о Вашей компании, ваши деловые партнеры или конкуренты могут использовать правоохранительные органы чтобы «свести счеты». Соблюдайте принятые обязательства, вовремя реагируйте на претензии и позаботьтесь о своей деловой репутации.

Мы рекомендуем назначить лицо, ответственное за управление настоящим протоколом. Это может быть и сам руководитель компании, работник ответственный за юридическое сопровождение, руководитель службы безопасности или член совета директоров. Допустимо привлечь для такой задачи адвоката или внешнего управляющего. При выборе следует руководствоваться здравым смыслом и наибольшим «центром компетенций», которые сосредоточены в вашей компании.

С уважением,
Михаил Викторович Черников, Ассоциация безопасности бизнеса и комплаенса
Адвокат Татьяна Анатольевна Тарахович