ТОП-6 основополагающих комплаенс-документов

13.08.2018 СТАТЬИ

Этой статьей открывается серия публикаций, посвященных противодействию мошенничеству в бизнесе посредством использования форензик-инструментов. Каждая статья будет представлять собой своего рода инструкцию по решению одной из задач: от построения системы комплаенса до расследования хищений и представления необходимых

доказательств в суде. К сожалению, многие компании не уделяют должного внимания превентивным мерам и вынуждены учиться на собственных ошибках, поэтому начнем с того, как выстроить внутренние процедуры и установить контроль над их исполнением, чтобы снизить количество неприятных инцидентов до минимума.

1 Комплаенс-политика

Комплаенс-политика — основополагающий внутренний документ, отражающий подход компании к соблюдению действующего российского и международного законодательства, внутрикорпоративных норм и правил делового этикета (1 Компании должны учитывать как минимум положения Федерального закона от 25.12.2008 № 273 «О противодействии коррупции», а также соответствующие нормы Уголовного кодекса РФ и Кодекса РФ об административных правонарушениях. Кроме того, в определенных случаях компании могут попадать под действие различных международных актов: FCPA, UK BA, Sapin II и др. Требование всех применимых к компании законодательных норм должно полностью учитываться в ее комплаенс-политике). Комплаенс-политика не должна носить декларативный характер: руководству необходимо назначать конкретных лиц, ответственных за исполнение ее положений, и каждый раз указывать на последствия их несоблюдения. Этот документ регламентирует такие бизнес-процессы, которые могут быть связаны с коррупционными или мошенническими действиями, а именно: наем сотрудников; взаимодействие с контрагентами и проверка их деловой репутации; взаимодействие с государственными органами; спонсорская и благотворительная деятельность, затраты на подарки и представительские расходы и пр.

Далее приведены внутрикорпоративные документы, на которые должна опираться комплаенс-политика организации.

2 Кодекс делового поведения

Кодекс делового поведения (Code of Conduct / Code of Ethics) — это свод правил, принципов и ценностей, которыми компания должна руководствоваться при ведении бизнеса. В нем устанавливаются стандарты делового и социального поведения и принятые в компании

этические нормы. По традиции Кодекс делового поведения является унифицированным документом, действие которого распространяется на все компании группы, независимо от места ведения бизнеса. Однако подобный подход не всегда оптимален, поскольку в некоторых странах положения данного документа необходимо адаптировать к особенностям местной культуры и бизнес-среды. Как показывает практика, кодекс, заимствованный из европейской штаб-квартиры и эффективно работающий на территории России и СНГ без всяких доработок, — это редкость.

3 Положение о комплаенс-офицере / комплаенс-службе

Ключевую роль в осуществлении контроля над соблюдением внутренней политики, в том числе в части комплаенса, играет комплаенс-офицер, а в расширенном варианте — комплаенс-служба компании.

Комплаенс-офицер должен быть независимым сотрудником и подчиняться непосредственно генеральному директору компании, совету директоров или комитету по этике (если такой имеется). Он отвечает за стандартизацию всех внутренних процедур, их регулярный аудит и проверку на соответствие постоянно изменяющемуся законодательству. Кроме того, именно комплаенс-офицеру приходят сообщении о различных нарушениях. Они должны быть рассмотрены им и переданы в соответствующий департамент для дальнейшего расследования или принятия мер. Еще одно важное направление деятельности комплаенс-офицера — информирование сотрудников компании обо всех нововведениях, касающихся требований комплаенса, а также проведение соответствующих тренингов.

В России комплаенс-офицера часто назначают из числа действующих сотрудников. Чаще всего это юрист, который совмещает комплаенс-функции со своими основными должностными обязанностями. Однако имеющийся опыт позволяет считать данную практику отрицательной в силу следующих причин:

> во-первых, комплаенс — это самостоятельный вид деятельности в компании, а значит,

занимающийся им сотрудник должен посвящать ему все свое рабочее время;

во-вторых, комплаенс-офицер должен быть лицом независимым и незаинтересованным.

4 Положение о работе горячей линии комплаенс

Одним из самых эффективных средств информирования о фактах мошенничества и прочих негативных инцидентах является горячая линия. Это канал, по которому сотрудники компании, контрагенты и даже третьи лица могут сообщать о любых известных им нарушениях. Существуют различные форматы горячей линии: телефон, email, форма обращения на сайте и другие, при этом можно одновременно использовать несколько из них.

Сейчас организации могут разрабатывать собственную горячую линию, использовать готовое решение или обращаться за подобной услугой к сторонним поставщикам. На рынке есть компании, предоставляющие услуги горячей линии в формате «24/7» с поддержкой нескольких языков, веб-интерфейсом, аналитикой по поступившим сообщениям и автоматической системой контроля, например: NAVEX Global, WhistleB, CSI Compliance Hotline.

Положение о работе горячей комплаенс-линии должно предусматривать анонимность всех поступающих сообщений, если, конечно, заявитель не пожелал обратного. В большинстве стран этот принцип строго регулируется законодательством о защите персональных данных.

В Положении должен быть определен порядок работы с обращениями, поступающими на горячую линию. Все обращения рассматриваются, передаются в соответствующий департамент, где по ним проводится расследование. Когда информация о нарушении подтверждается, к лицам, имеющим отношение к данному инциденту, применяются определенные санкции. Если речь идет о сотрудниках компании, то дело может дойти до увольнения и судебного разбирательства.

Демонстрация результатов расследования обращений является важным элементом

в продвижении горячей линии среди сотрудников компании и контрагентов. Информация о привлечении к ответственности виновного сотрудника или реализация изменений в работе компании на основе обращения отлично мотивирует на использование данного канала в целях информирования руководства об имеющихся проблемах и нарушениях. Положение о работе горячей линии должно предусматривать порядок обработки, хранения и защиты всех получаемых сведений.

Одной из типичных ошибок в компаниях, находящихся на территории СНГ, является получение информации по горячей линии сотрудниками службы безопасности и выборочное реагирование на поступающие сообщения. Также часто имеет место нарушение порядка работы с поступающей информацией, когда она передается как раз тому руководителю, на которого и жалуется сотрудник. Грамотно составленное Положение о работе горячей комплаенс-линии исключает подобные ситуации.

5 Положение о работе с контрагентами

Положение о работе с контрагентами содержит рекомендации по процедуре их приема и последующей работе с ними независимо от департамента компании. В данном документе детально прописывается, как должна проходить первичная или очередная (например, ежегодная) проверка контрагента: какую информацию следует у него запрашивать, к кому в компании нужно обращаться для проведения такой проверки, какие инструменты использовать при этом. Более того, согласно требованиям ФНС российские компании обязаны соблюдать принцип должной осмотрительности и проверять контрагентов перед заключением договоров. В Положении о работе с контрагентами должны быть указаны все публичные источники и автоматизированные инструменты проверки благонадежности контрагента, которыми пользуется компания.

Положение может предусматривать требования к мониторингу платежей контрагентам со стороны финансового департамента компании. С точки зрения форензик-подхода существует несколько десятков критериев подозрительности платежей, позволяющих снизить риск мошенничества и сделать работу с контрагентами более прозрачной.

В настоящее время многие компании внедряют системы автоматизированного контроля над подозрительными транзакциями в рамках существующих ERP-систем (такие возможности есть, например, в «1С», SAP и Oracle) и на базе решений сторонних разработчиков (SAS, Ditrix и др.). Хорошей практикой является наличие в Положении оговорки об аудите в соглашениях с контрагентами. Это позволяет подтверждать предоставленную контрагентом информацию о деловой благонадежности и соответствии требованиям применимого антикоррупционного законодательства.

Положение также должно предусматривать меры дисциплинарной ответственности сотрудников компании за неисполнение предусмотренных в нем требований.

6 Положение о работе с информацией

Основой эффективного противодействия мошенничеству является своевременный и легальный доступ к информации. Специалистов по предотвращению хищений интересуют сведения о деятельности компании, протекании в ней бизнеспроцессов, коммуникации сотрудников и контрагентов. Информация, поступающая из разных источников, создает детальное представление о работе организации. Пользуясь ИТ-инфраструктурой работодателя, сотрудники могут вести личную переписку, хранить личные документы и персональные данные, то есть обрабатывать охраняемую законом информацию. Для того чтобы иметь доступ ко всей информации на устройствах и в информационных системах, принадлежащих компании, и при этом минимизировать риск нарушения законодательства, нужно установить внутренние правила работы с информацией и ИТ-инфраструктурой.

Положение о работе с информацией должно предусматривать:

- явный запрет на использование работниками ИТ-систем и оборудования компании в личных целях, в том числе на хранение в компьютерах личной информации и ведение личной переписки;
- закрепление за компанией права собственности на всю информацию, хранимую

и обрабатываемую в ее ИТ-инфраструктуре;

- право компании контролировать соблюдение сотрудниками правил работы в ИТ-инфраструктуре и проводить проверки;

- получение от проинформированного сотрудника согласия на обработку персональных данных, в том числе с целью контроля соблюдения внутренней политики компании, а также качества и полноты выполнения им своих должностных функций;

- обязанность компании надлежащим образом хранить и защищать персональные данные сотрудников и контрагентов, равно как и обязанность сотрудников и контрагентов сохранять коммерческую тайну компании в неприкосновенности.

Наличие указанных пунктов в Положении позволяет контролирующим подразделениям организации в случае необходимости проведения корпоративного расследования получать и анализировать информацию с корпоративных устройств и ИТ-систем компании, а затем использовать ее в качестве источника доказательств.

При разработке внутренних нормативных документов, касающихся работы с персональными данными сотрудников и контрагентов, а также защиты такой информации (например, Положения о горячей комплаенс-линии) необходимо учитывать нормы российского и международного законодательства о защите персональных данных. Так, в мае 2018 г. вступит в силу GDPR — Европейский регламент защиты персональных данных. Многие иностранные компании, работающие в Российской Федерации, уже учли предусмотренные им требования при разработке соответствующих комплаенс-документов (См.: Антипов И. General data protection regulations: новые вызовы для бизнеса // Legal Insight. — 2017. — № 8).

Информирование о нормах комплаенс

Важно, чтобы все сотрудники компании знали и понимали нормы комплаенса. Лучшими способами информирования об этом внутри компании являются:

- прямая коммуникация со стороны непосредственного руководства;
- корпоративный веб-сайт, корпоративные СМИ;
- комплаенс-тренинги с элементами деловых игр.

Ко всем указанным способам применимо общее важное требование — периодичность их применения. Информирование должно происходить постоянно и на всех уровнях деятельности компании. Каждый раз по результатам информирования обязательно должно проводиться тестирование, результаты которого, тем не менее, не стоит привязывать к каким-либо поощрительным или, напротив, репрессивным мерам, чтобы не вызвать у сотрудников нервозности.

Самыми эффективными с точки зрения возможностей количественного и географического охвата являются онлайн-тренинги с последующим ситуативным тестированием (использование решений на платформах ISpring Online, Webinar / Comdi, Websoft, «Мираполис» и др.). Последний тренд — это чат-боты, реализованные на платформах корпоративных средств коммуникации либо на базе общеизвестных мессенджеров (Telegram, WhatsApp, Skype).

После информирования и тестирования сотрудников на предмет понимания норм комплаенса можно формально закрепить сформированное у них намерение следовать указанным нормам. Ознакомление с соответствующим документом под роспись является простым способом официально подтвердить, что сотрудник прочитал его и обязуется руководствоваться им в своей работе.

Для формирования эффективной системы противодействия мошенничеству также

необходимо, чтобы стиль работы высшего руководства задавал соответствующий тон поведению всех остальных сотрудников. Каким бы банальным это ни казалось, но если менеджмент не придерживается тех же правил, что предусмотрены для работников компании, то без этого tone from the top, система работать не будет.

Вовлеченность руководителей в процесс противодействия корпоративному мошенничеству наиболее эффективно демонстрируют их регулярные публикации на внутренних ресурсах компании и встречи с сотрудниками для обсуждения вопросов, связанных с неэтичным поведением. Подобные беседы целесообразно проводить каждые три месяца и на конкретных примерах разъяснять, как выявляется конфликт интересов, что с этим нужно делать и каковы негативные последствия для тех, кто целенаправленно нарушал антикоррупционную политику.

Статья опубликована в Legal Insight №1, 2018.

Александр Хаки — исполнительный директор CSI Group

Николай Сметанин — менеджер CSI Group

СТАТЬИ