

КОРПОРАТИВНОЕ ИНФОРМАТОРСТВО КАК ЭЛЕМЕНТ СИСТЕМЫ КОРПОРАТИВНЫХ ОТНОШЕНИЙ

Дмитрий Текутьев¹

8.1. Суть и назначение корпоративного информаторства

Whistleblowing (доносительство, осведомительство, информаторство, оповещение)² – доведение до руководства информации о незаконных, мошеннических, небезопасных или аморальных действиях, совершаемых в государственных организациях или частных компаниях³. Термин впервые был использован в США в 1970-х годах в качестве обозначения заявлений о коррупции. Его появление связывают с именем американского активиста и адвоката по делам о защите прав потребителей Р. Надера, который в 1972 году на конференции по вопросам профессиональной ответственности определил

¹ Текутьев Дмитрий Иванович, кандидат юридических наук, доцент факультета права НИУ «Высшая школа экономики».

² Термин «whistleblowing» происходит от англоязычного сочетания «to blow the whistle», что буквально переводится как «дуть в свисток». Поскольку его можно назвать устоявшимся в профессиональной среде, в данной главе используются как английский термин, так и его русские синонимы.

³ International Principles for Whistleblower Legislation Best Practices for Laws to Protect Whistleblowers and Support Whistleblowing in the Public Interest.

«whistleblowing» как действие человека, который, полагая, что общественные интересы приоритетнее интересов организации, где он работает, сообщает о том, что организация вовлечена в коррупционную, незаконную, мошенническую или причиняющую вред обществу деятельность¹.

Информаторство может иметь место как в государственных структурах (public sector whistleblowing), так и в частных компаниях (public sector whistleblowing или corporate whistleblowing). Применительно к корпоративным отношениям термин «whistleblowing» был предложен М.П. Мичели и Ж.П. Ниаром в 1992 году. Под ним они понимали раскрытие бывшими или действующими работниками организации противоправных, аморальных или незаконных действий, совершаемых под контролем их работодателей, в пользу лиц или органов, способных предотвратить подобные действия². Предмет изучения данной главы – корпоративный whistleblowing как элемент системы корпоративных отношений, а также проблемы и вызовы, с которыми корпорации могут столкнуться при внедрении данной практики.

На сегодняшний день интеграция в систему корпоративного управления практик и механизмов whistleblowing рассматривается в профессиональной литературе и международных документах как важный аспект системы комплаенса, управления рисками и внутреннего контроля в организации³. В частности, выделяются следующие функции корпоративного информаторства.

¹ См.: Vandekerckhove W. Whistleblowing and Organizational Social Responsibility: A Global Assessment // Ashgate Publishing Company, 2006. P. 8.

² Miceli M., Near J. Blowing the Whistle: the Organisational and Legal Implications for Companies and Employees. New York: Lexington Books, 1992. P. 15.

³ См., например, Lombard S., Brand V., Austin J. Corporate Whistleblowing Regulation: Theory, Practice, and Design (Springer, 2019); Brand V., Lombard S. Good Governance Practice in Relation to Corporate Whistleblowing // Governance Directions. 2015. №67 (1); Near J.P., Dworkin T.M. Responses to Legislative Changes: Corporate Whistleblowing Policies // Journal of Business Ethics. 1998. № 17 (14); Hassink H., Vries M. de, Bollen L. A Content Analysis of Whistleblowing Policies of Leading European Companies // Journal of Business Ethics. 2007.

- Whistleblowing является одним из средств минимизации агентской проблемы в корпорации. Агентская проблема, суть которой заключается в риске оппортунистического поведения менеджмента в условиях информационной асимметрии, остается одной из наиболее дискутируемых в правовой и управленческой литературе уже несколько десятилетий¹. Ключевым фактором, порождающим агентскую проблему, является наличие информационной асимметрии² в отношениях менеджмент – акционеры и менеджмент – совет директоров. Осуществляя операционное управление корпорацией в каждодневном режиме, исполнительные директора не только объективно обладают подробной информацией о том, что на самом деле происходит в компании, но и склонны не допускать распространения негативной информации. В этой ситуации наличие у акционеров или совета директоров канала обратной связи в виде сообщения сотрудников (а также иных стейкхолдеров, обладающих полезной информацией о происходящих внутри организации процессах, например контрагентов) является средством преодоления информационной асимметрии, помогающим принципалам получить сведения об использовании недобросовестных практик в деятельности агентов.

- Corporate whistleblowing помогает корпорациям самостоятельно выявлять возникающие нарушения законодательства и оперативно реагировать на них,

№ 75 (1); *Ebersole D. Blowing the Whistle on the Dodd-Frank Whistleblower Provisions // Ohio State Entrepreneurial Business Law Journal. 2007. № 75 (1); Lee G., Fargher N. Companies' Use of Whistle-Blowing to Detect Fraud: An Examination of Corporate Whistle-Blowing Policies // Journal of Business Ethics. 2013. № 114 (2). P. 283, 285.*

¹ См., например, *Berle A., Means G. The Modern Corporation and Private Property. New York: Macmillan, 1932. Jensen M., Meckling W. Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure // Journal of Financial Economics. 1976. Vol. 3. № 4.*

² Информационная асимметрия – ситуация, когда одни участники рынка владеют большей (или лучшей) информацией, чем другие, и могут использовать это в своих интересах (см.: *Макконнелл К.Р., Брю С.Л. Экономикс: принципы, проблемы и политика. М.: Республика, 1992. Т. 1. С. 88).*

не прибегая к помощи государства¹. Эффективно работающая система корпоративного информаторства выгодна как компании, так и государству, поскольку позволяет экономить корпоративные и государственные ресурсы на выявление и расследование различных правонарушений. По сути, руководство корпорации при поступлении от сотрудника информации о нарушениях становится своеобразным судом первой инстанции, который может оперативно и с минимальными издержками отреагировать на «иск» и в зависимости от обстоятельств дать или не дать делу дальнейший ход. К примеру, как отмечается в отчете Ассоциации сертифицированных специалистов по борьбе с мошенничеством (ACFE), включающем данные по 96 странам, в 2022 году 43% всех корпоративных мошенничеств были раскрыты именно благодаря информаторам².

- Информирование на раннем этапе о недобросовестных практиках позволяет решить проблему на корню, то есть принять превентивные меры, пока она не приобрела системный или массовый характер. Если в компании существуют недобросовестные практики, а система их доведения до руководства (internal whistleblowing) отсутствует или не работает, велика вероятность, что рано или поздно сотрудник прибегнет к внешним каналам распространения информации (external whistleblowing), например, обратившись к регулятору, в правоохранительные органы или СМИ. Чем более системная и запущенная проблема, тем выше риск того, что информация о ней станет публичной. Проникнув в медиа, подобные сведения могут принести компании большие репутационные убытки, что в конечном счете отразится на цене ее акций³.

¹ Обычно для обозначения данного явления в англоязычной литературе используется термин «private enforcement», с противопоставлением его термину «public enforcement», то есть различным мерам государственного принуждения.

² Association of Certified Fraud Examiners, Report to the Nations, 2022 under Key Findings, available at <https://www.acfe.com/fraud-resources/report-to-the-nations-archive>

³ При этом, как показывают исследования, внешнее информирование является более эффективным средством, чем внутреннее. В частности, 44% информаторов по внешним каналам сообщили,

- Информаторство является одним из элементов системы управления рисками, информационной прозрачности и устойчивого развития корпорации в целом. В последние годы преобладающей тенденцией в корпоративной политике стало соответствие принципам устойчивого развития и критериям ESG (Environmental, Social, Governance), в связи с чем компаниям предъявляется все больше требований по ответственному ведению бизнеса со стороны государства, общества, инвесторов и широкого круга иных стейкхолдеров. Факторами ESG являются отсутствие в компании недобросовестных практик, коррупции, нарушения законодательства: эффективная защита прав работников; информационная прозрачность. Следовательно, наличие в компании процедур информирования о недобросовестном поведении менеджмента – гарантия того, что любые несоответствия принципам ESG будут своевременно выявлены и доведены до сведения руководства. Это делает корпоративное управление и бизнес компании в целом более устойчивым к рискам, которые при отсутствии информирования просто не принимались бы во внимание¹.

что в результате их обращения проблема была решена, и 27% респондентов заявили, что внутреннее информирование дало результат (см.: *Rothschild J., Miethe T.D.* Whistleblower Disclosures and Management Retaliation // *Work and Occupations*. 1999. № 26 (1). P. 107–128; *Dworkin T.M., Baucus M.S.* Internal vs. External Whistleblowers: A Comparison of Whistleblowing Processes // *Journal of Business Ethics*. 1998. № 17 (12). P. 1281–1298).

¹ В зарубежной литературе имеется ряд эмпирических исследований, подтверждающих связь между внедрением процедур внутреннего информирования и повышением уровня корпоративного управления (см., например, *Stubben S.R., Welch K.T.* Evidence on the Use and Efficacy of Internal Whistleblowing Systems // *Journal of Accounting Research*. 2020. № 58 (2). P. 473, 513).

8.2. Мировой опыт законодательного регулирования корпоративного информаторства

Законодательная защита корпоративных информаторов – относительно новое явление: первые подобные законы появились в США и странах Западной Европы в конце 1990-х – начале 2000-х годов. Однако эта практика получила широкое распространение, и по состоянию на конец 2018 года законы, предусматривающие те или иные меры защиты корпоративных информаторов, были приняты в более чем 50 государствах¹. В силу ограниченности объема настоящей главы автор анализирует опыт регулирования данного явления только в корпоративном праве Великобритании, США, Европейского союза и России.

8.2.1. Великобритания

Великобритания стала одной из первых стран, в которой защита информаторов была закреплена на законодательном уровне после принятия в 1998 году Закона о раскрытии информации в общественных интересах (Public Interest Disclosure Act, PIDA)². Статья 1 указанного закона вводит термин «защищенное информирование» (protected disclosure), под которым понимается защита сотрудника³ от негативных последствий раскрытия информации о работодателе, если такая информация касается:

- совершения преступления;
- нарушения законодательства;

¹ См.: Whistleblowing protection: Global Guide (Freshfields Bruckhaus Deringer, 2018). Полный текст документа доступен по ссылке: <https://www.freshfields.com/49f7fd/globalassets/services-page/people-and-reward/whistleblower-protection-global-guide-may-2019.pdf>

² Полный текст закона доступен по ссылке: <https://www.legislation.gov.uk/ukpga/1998/23/contents>

³ Положения PIDA распространяются на всех работников как в частном, так и в государственном и некоммерческом секторах Соединенного Королевства. Действие закона распространяется на исполнителей по гражданско-правовым договорам, стажеров, консультантов, домашних работников, а также иных специалистов, получающих вознаграждение на легальном основании (S.43K PIDA).

- риска для здоровья или безопасности человека;
- причинения ущерба окружающей среде;
- преднамеренного сокрытия информации, относящейся к любому из вышеперечисленных пунктов.

Важно отметить, что, согласно первоначальной редакции PIDA, такое раскрытие информации должно быть сделано из добросовестных побуждений (in good faith), то есть при отсутствии недобросовестных мотивов или мотива личной выгоды и с убеждением, что нераскрытие сведений негативно скажется на деятельности компании-работодателя. Однако в 2013 году данный критерий был исключен из текста закона, кроме случаев, когда определяется размер компенсации морального ущерба сотруднику, который может быть снижен, если он раскрыл информацию из недобросовестных мотивов. В настоящее время в Великобритании защита предоставляется информаторам независимо от мотивов раскрытия, если только представленные ими сведения не являются ложными¹.

Статья 5 PIDA гарантирует информаторам следующие средства защиты:

- право подать иск в любой суд по трудовым спорам о несправедливом увольнении в случае расторжения трудового договора с ними в результате раскрытия информации;
- право на восстановление на работе и компенсацию в случае обоснованной жалобы на несправедливое увольнение;
- право на компенсацию морального ущерба;
- право на защиту от возмездия со стороны работодателя в виде отказа в продвижении по службе и иных форм дискриминации.

Другой существенной особенностью защиты корпоративных информаторов в Великобритании является то, что PIDA отменяет действие любых оговорок о конфиденциальности (gagging clauses), содержащихся в трудовых договорах и соглашениях о прекращении

¹ См.: Whistleblowing as a Corporate Governance Mechanism: A Comparative Analysis of Employee-Whistleblower Protection in the United Kingdom and Nigeria. 2020. Available at SSRN: <https://ssrn.com/abstract=3547899> or <http://dx.doi.org/10.2139/ssrn.3547899>

трудовых отношений, в той мере, в какой они противоречат положениям данного закона. Таким образом, PDA косвенно запрещает работодателю использовать оговорки о конфиденциальности в трудовых договорах с целью заставить сотрудников молчать и помешать разглашению информации об имеющихся в компании недобросовестных практиках.

8.2.2. Соединенные Штаты Америки

В США защита информаторам в частном секторе предоставлена позднее, чем в Великобритании, хотя соответствующие меры в публичном секторе были введены еще в 1989 году согласно Закону о защите информаторов (Whistleblower Protection Act 1989)¹. Импульсом к развитию законодательства о правовой защите корпоративных информаторов стало принятие в США в 2002 году Закона Сарбейнса–Оксли (The Sarbanes–Oxley Act, SOX)², который явился реакцией на серию банкротств и корпоративных скандалов в крупнейших американских корпорациях, вызванных недобросовестным поведением топ-менеджмента. В Законе Сарбейнса–Оксли защите корпоративных информаторов посвящены ст. 806 и 1107. Согласно ст. 806 названного закона:

А) компания, выпускающая ценные бумаги, а также любой ее сотрудник, работник, подрядчик, субподрядчик или агент не могут уволить, понизить в должности, отстранить от работы, угрожать, преследовать или иным образом дискриминировать сотрудника, который в соответствии с данным законом:

- предоставляет информацию;
- способствует предоставлению информации;
- иным образом помогает в расследовании любых действий, которые, по обоснованному мнению сотрудника, представляют собой нарушение федерального закона, актов Комиссии по ценным бумагам и биржам или любого другого акта, касающегося нарушения прав акционеров.

¹ Полный текст закона доступен по ссылке: <https://www.govinfo.gov/content/pkg/STATUTE-103/pdf/STATUTE-103-Pg16.pdf>

² Полный текст закона доступен по ссылке: <https://www.govinfo.gov/content/pkg/COMPS-1883/uslm/COMPS-1883.xml>

Б) 1. Работник, который подвергся увольнению или другой форме дискриминации со стороны любого лица в нарушение подраздела А, может защитить свои права путем:

- подачи жалобы в Министерство труда США;
- подачи иска в соответствующий окружной суд США.

2. Работник, выигравший любой иск, согласно подразделу Б-1, имеет право на все дальнейшие средства правовой защиты, в том числе:

- восстановление в должности с тем же стажем, который работник имел бы, если бы дискриминация в отношении его не имела места;
- сумму заработной платы с процентами за весь период нахождения без работы;
- компенсацию за любой иной ущерб, понесенный в результате дискриминации, включая судебные издержки, оплату услуг экспертов и гонорары адвокатов.

Статья 1107 Закона Сарбейнса – Оксли устанавливает административную и уголовную ответственность в виде штрафа или лишения свободы на срок до 10 лет за любые умышленные действия работодателей, наносящие вред информаторам и вызванные желанием отомстить за распространение правдивой информации о положении дел в компании.

Нормы о защите корпоративных информаторов в США содержатся в регулирующей деятельность корпораций на рынке ценных бумаг и принятом в 2010 году Законе о реформировании Уолл-стрит и защите прав потребителей, также именуемом Законом Додда – Франка (Dodd – Frank Wall Street Reform and Consumer Protection Act)¹.

Согласно ст. 922 Закона Додда – Франка, Комиссия по ценным бумагам и биржам (далее – SEC) обязана выплатить финансовое вознаграждение информаторам, добровольно предоставившим SEC информацию, которая помогла регулятору успешно расследовать правонарушение, в размере не менее 10% и не более 30% от общей суммы денежных санкций, наложенных

¹ Полный текст закона доступен по ссылке: <https://www.cftc.gov/LawRegulation/DoddFrankAct/index.htm>

на правонарушителя в соответствии с иском. Конкретный размер вознаграждения информатора в рамках указанного коридора определяется по усмотрению SEC с учетом значимости предоставленных сведений для успеха дела и степени помощи, оказанной информатором и любым его законным представителем при расследовании дела.

8.2.3. Страны Европейского союза

На уровне Европейского союза действует Директива 2019/1937/ЕС Европейского парламента и Совета ЕС от 26 ноября 2019 года о защите лиц, сообщающих о нарушениях законодательства Европейского союза¹ (далее – Директива ЕС), – официальное распоряжение для стран-членов, запрещающее преследование информаторов и подлежащее исполнению через принятие соответствующих национальных законов. Главная цель Директивы ЕС – обеспечение единого стандарта защиты информаторов, действующего на территории всех стран Европейского союза (далее – ЕС). Согласно документу каждое из государств – членов ЕС должно было до 17 декабря 2021 года внедрить требования Директивы ЕС в свои национальные правовые и институциональные системы.

Директива ЕС запрещает прямое или косвенное преследование сотрудников-информаторов (как действующих, так и бывших) в государственном и частном секторах. В частности, информаторы должны быть защищены от корпоративных исков за убытки, причиненные в результате их деятельности. Помимо этого, государство обязано предоставить им психологическую поддержку для преодоления стресса, связанного с оказываемым на них давлением. Документ также предусматривает необходимость предоставления защиты лицам, которые находятся с информатором в семейных, деловых или любых иных отношениях в случае, если существует вероятность нарушения их прав из-за раскрытия информации заявителем.

¹ Полный текст закона доступен по ссылке: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019L1937>

Директива ЕС рекомендует сотрудникам информировать о нарушениях в первую очередь через внутренние каналы в компании. Прибегать к сообщению по внешним каналам или раскрывать сведения публично рекомендуется только в случае, если внутренние каналы отсутствуют либо обращение не принесло результатов, а также если велика вероятность ответных действий репрессивного характера со стороны руководства. Тем не менее решение о выборе канала сообщения должно оставаться на усмотрение информатора.

8.2.4. Российская Федерация

В России защита информаторов регулируется главным образом антикоррупционным, а также уголовно-процессуальным законодательством. Согласно ч. 4 ст. 9 Федерального закона «О противодействии коррупции»¹, государственный или муниципальный служащий, уведомивший представителя нанимателя (работодателя), органы прокуратуры или другие государственные органы о фактах обращения в целях склонения его к совершению коррупционного правонарушения, совершения другими государственными или муниципальными служащими коррупционных правонарушений, непредставления сведений, представления заведомо неполных сведений, за исключением случаев, установленных федеральными законами, либо представления заведомо недостоверных сведений о доходах, об имуществе и обязательствах имущественного характера, находится под защитой государства в соответствии с законодательством Российской Федерации. Защита таких лиц регулируется Федеральным законом «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»². В частности, ст. 5 данного закона предусматривает следующие меры защиты информаторов:

- личная охрана, охрана жилища и имущества;

¹ Федеральный закон от 25 декабря 2008 года № 273-ФЗ «О противодействии коррупции».

² Федеральный закон от 20 апреля 1995 года № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов».

- выдача оружия, специальных средств индивидуальной защиты и оповещения об опасности;
- временное помещение в безопасное место;
- обеспечение конфиденциальности сведений о защищаемых лицах и об их имуществе;
- перевод на другую работу (службу), изменение места работы (службы) или учебы;
- переселение на другое место жительства;
- замена документов, изменение внешности.

Важно отметить, что данные меры защиты распространяются только на государственных и муниципальных служащих и не распространяются на иных информаторов.

Защита информаторов и иных лиц, оказывающих помощь следствию, регулируется Уголовно-процессуальным кодексом Российской Федерации¹, Федеральным законом «Об оперативно-розыскной деятельности»² и Федеральным законом «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»³. В русскоязычной юридической литературе понятие «whistleblower» также рассматривается преимущественно в контексте мер по борьбе с коррупцией и переводится в большинстве случаев – «заявитель или информатор о коррупционных правонарушениях»⁴. Однако чаще всего для обозначения

¹ Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 года № 174-ФЗ.

² Федеральный закон от 12 августа 1995 года № 144-ФЗ «Об оперативно-розыскной деятельности».

³ Федеральный закон от 20 августа 2004 года № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства».

⁴ См., например, *Балог М.М.* Противодействие коррупции в России: защита заявителей // Вестник Псковского государственного университета. Серия: Экономика. Право. Управление. 2018. № 8. С. 39–44; *Волосова Н.Ю., Журкина О.В.* К вопросу о программе защиты разоблачителей (информаторов) по делам коррупционной направленности // Всероссийский криминологический журнал. 2018. Т. 12. № 5; *Спектор Е.И., Севальнев В.В.* Вопросы правовой защиты лиц, сообщающих о фактах коррупции // Журнал зарубежного законодательства и сравнительного правоведения. 2015. № 4; *Макарова О.В.* Обеспечение безопасности лиц, способствующих предупреждению и раскрытию коррупционных

ния информирования о коррупции используется другой иностранный термин «денунциация»¹.

Защита корпоративных информаторов российским законодательством не регулируется. Для защиты от дискриминации со стороны руководителя или коллег в связи с информированием работник может обратиться в суд или комиссию по трудовым спорам на основании общей нормы ст. 3 Трудового кодекса Российской Федерации² (далее – ТК РФ) о запрете дискриминации. В частности, увольнение сотрудника в результате дискриминации может повлечь за собой обязанность работодателя восстановить его на работе (ст. 396 ТК РФ), выплатить ему среднюю заработную плату за время вынужденного простоя (ст. 157 ТК РФ), а также возместить прочие убытки и расходы, в том числе компенсировать моральный вред (ст. 394 ТК РФ).

Рекомендательные акты уделяют чуть больше внимания данной проблеме, причем в отдельных документах Банка России употребляется даже англоязычный термин «whistleblowing»³. К примеру, Кодекс корпоративного управления Российской Федерации⁴ (далее – Кодекс) в п. 261 рекомендует публичным организациям организовать в рамках системы управления рисками и внутреннего контроля безопасный,

преступлений // Журнал российского права. 2015. Т. 3. № 7. С. 97–105; *Шевурдяев С.Н.* Концептуальные пробелы в системе российского антикоррупционного законодательства // Вестник Саратовской государственной юридической академии. 2020. № 1. С. 121–131.

¹ См., например, *Батищева Н.А.* Понятие «whistleblowers» и проблема защиты информаторов о преступлениях в европейской правовой культуре // Право и практика. 2021. № 1; *Трофимов Е.В.* Антикоррупционная денунциация: методологические проблемы, зарубежный опыт и российские перспективы // Административное и муниципальное право. 2021. № 4.

² Трудовой кодекс Российской Федерации от 30 декабря 2001 года № 197-ФЗ.

³ См., например, информационное письмо от 17 декабря 2019 года № ИН-06-39/93 «Информационное письмо о разработке и внедрении кодексов этики финансового аналитика».

⁴ Письмо Банка России от 10 апреля 2014 года № 06-52/2463 «О Кодексе корпоративного управления».

конфиденциальный и доступный способ (горячую линию) информирования совета директоров (комитета совета директоров по аудиту) и подразделения внутреннего аудита о фактах нарушений законодательства, внутренних процедур, кодекса этики общества любым его работником и (или) любым членом органа управления или органа контроля за финансово-хозяйственной деятельностью общества. В Кодексе оговорено, что лицо, предоставившее соответствующую информацию, должно быть защищено от любых форм давления (в том числе от увольнения, преследования и других форм дискриминации).

В другом рекомендательном документе, Руководстве для членов совета директоров финансовой организации¹, Банк России выделяет в числе функций совета директоров формирование в организации эталонных стандартов корпоративной культуры, в том числе направленных на предотвращение рисков недобросовестного поведения, а также внедрение практик по предотвращению рисков недобросовестного поведения сотрудников организации. В этом же документе в числе функций комитета совета директоров по аудиту предусмотрен контроль эффективности функционирования системы оповещения о потенциальных случаях недобросовестных действий работников организации и третьих лиц, а также об иных нарушениях.

Таким образом, Россию можно отнести к числу стран, где защита информаторов распространяется только на публично-правовые отношения (главным образом антикоррупционные и уголовно-правовые), в то время как специальное законодательное регулирование защиты корпоративных информаторов отсутствует. Вместе с тем в данной области имеются рекомендательные нормы, разработанные Банком России.

¹ Информационное письмо Банка России от 28 февраля 2019 года № ИН-06-28/18 «О руководстве для членов совета директоров (наблюдательного совета) финансовой организации».

8.3. Лучшие практики внедрения института корпоративного информаторства

Создание эффективной и реально действующей системы информирования о недобросовестных практиках в корпорациях не является простой задачей. Во-первых, как было продемонстрировано выше, далеко не во всех странах меры защиты корпоративных информаторов закреплены на уровне законодательства. Во-вторых, даже там, где действуют законы о защите информаторов, на практике защитить их интересы и создать стимулы к информированию не всегда получается. В частности, в отчете юридической компании Freshfields Bruckhaus Deringer 2018 года отмечается: несмотря на гарантии, установленные PIDA, почти две трети британских менеджеров среднего звена избегают практики whistleblowing из-за страха навредить своей карьере.

Помимо этого, согласно данному отчету, около 55% сотрудников считают: они не смогут сохранить анонимность, если раскроют негативную информацию о положении дел в компании, что служит дополнительным сдерживающим фактором¹. Соответственно, для того, чтобы информаторы не опасались сообщать сведения, необходимо не только закрепить механизмы их защиты на законодательном уровне, но и выстроить эффективные процедуры информирования и средства последующей защиты информаторов прежде всего на уровне отдельной корпорации. Локальный уровень является первым эшелом выявления недобросовестных практик и защиты информаторов, который может работать, даже если в законодательстве страны отсутствуют специальные меры защиты.

Главная проблема на локальном уровне заключается в том, что менеджмент компании, не заинтересованный в разглашении информации об используемых им недобросовестных практиках, склонен принимать различные меры по противодействию информаторам. Подобные меры могут включать:

¹ См.: <https://www.financierworldwide.com/whistleblowing-in-the-uk-feb18#.Xh8GxMhKg2w>

- стремление не документировать как сообщение информатора, так и собственные обещания принять меры по исправлению ситуации и иные заверения с целью их последующего опровержения или отрицания;
- попытки отговорить информатора от распространения сведений, мотивируя это тем, что расследование повредит отношениям внутри коллектива, имиджу организации, повлечет для нее серьезные финансовые издержки и т.д.;
- желание не давать делу ход и не выпускать негативную информацию за пределы организации или ее внутреннего подразделения;
- попытки оказать давление на свидетелей, а также привлечь свидетелей, опровергающих данные, поступившие от информатора, или утверждающих, что информатор сам виновен в произошедшем;
- затягивание процесса расследования, а также замалчивание его результатов;
- в случае если дело доходит до суда – затягивание судебного процесса с целью истощить истца морально и финансово в ходе длительного разбирательства;
- дискредитация информатора, стремление подорвать его уверенность в своей правоте и психологическое состояние в целом;
- моббинг (mobbing) – попытки изолировать информатора от коллег и вышестоящего руководства, а также настроить против него коллег путем распространения порочащих его слухов, сплетен, инсинуаций и т.д.
- обвинение жертвы (victim-blaming) – стремление установить в ходе официального расследования вину информатора в происходящих нарушениях и представить ситуацию таким образом, чтобы публично все выглядело как его попытка замести следы;
- газлайтинг (gaslighting) – манипуляции, когда менеджмент стремится выставить информатора как неадекватного или психически нездорового человека, стремящегося найти проблемы там, где на самом деле они отсутствуют;
- угрозы применения к информатору дисциплинарных санкций в случае распространения сведений или обещание продвижения по службе в случае их нераспространения.

Кейс компании General Motors (2002)¹

В ноябре 2001 года сотрудник General Motors (далее – GM) Кортланд Келли обнаружил дефект в системе зажигания автомобилей серии Chevrolet Cobalt, выпускаемых GM. Дефектный замок зажигания этой серии в любой момент мог переключиться в положение «выключено» и отключить питание, а также подушки безопасности именно тогда, когда они больше всего необходимы.

Информатор сообщил о проблеме своему вышестоящему руководителю, который ответил, что разделяет опасения Келли, однако отзыв серии с рынка будет слишком дорогостоящим для компании. Тогда Келли решил пойти дальше и в служебной записке, адресованной начальнику своего босса, Киту Маккензи, директору по качеству автомобильных марок, прямо указал, что, по его мнению, GM нарушает закон, не решая должным образом проблемы с безопасностью автомобилей Chevrolet Cobalt.

В апреле 2002 года GM отозвала с рынка партию в 60 тыс. неисправных автомобилей, однако Келли был переведен на должность бренд-менеджера, не связанную с проверкой качества, после чего его карьера в компании пошла по наклонной. По словам информатора, такими действиями ему дали понять, что не одобряют его активность.

В 2003 году Келли подал в суд на GM за задержку в принятии мер по устранению неполадок в автомобилях, но в итоге проиграл дело. Как утверждал информатор, во время дачи показаний юрист GM оказывал на него давление, заставляя его признать, что высказывание опасений по поводу безопасности автомобилей не входило в его должностные обязанности.

¹ Описание кейса приводится по материалам статьи «GM Recalls: How General Motors Silenced a Whistle-Blower» на официальном сайте агентства Bloomberg.
<https://www.bloomberg.com/news/articles/2014-06-18/gm-recalls-whistle-blower-was-ignored-mary-barra-faces-congress>

История с Келли неожиданно получила продолжение в 2014 году, когда в свет вышел отчет прокурора Энтони Валукаса, в котором на основании интервью со свидетелями и анализа документов утверждалось, что не устраненная в 2002 году неисправность в автомобилях марки Chevrolet Cobalt связана как минимум с 13 смертями и 54 авариями. Отчет Валукаса обвинял компанию GM в более чем десятилетней задержке, прежде чем компания отозвала неисправные автомобили. В качестве основной причины бездействия указывались корпоративная бюрократия, фатально безразличная к растущим доказательствам того, что автомобили GM небезопасны. Хотя каждый был обязан устранить проблему, никто не взял на себя ответственность. Однако, как отмечали некоторые сотрудники, на деле ситуация была еще хуже – проблемы GM выходили за рамки простого бездействия или безразличия менеджмента – выражение своего мнения работниками активно не поощрялось. В частности, на странице 93 отчета Валукаса приводится цитата инспектора по безопасности GM Стивена Окли, который утверждал, что он боялся настаивать на наличии проблем с безопасностью автомобилей Chevrolet Cobalt после того, как увидел, что его предшественника Келли «выгнали с работы за то, что он именно так и поступил». По его словам, поступок Келли имел обратный эффект: его проигрыш в суде и то, как после этого застопорилась его карьера, научили других сотрудников компании молчать.



Ниже представлен ряд лучших практик по внедрению института корпоративного информаторства и защиты информаторов, которые можно выделить в результате обобщения норм законодательства ведущих зарубежных стран, а также положений рекомендательных документов. Главным из них являются Руководящие принципы G20 по обеспечению эффективной защиты информаторов (G20 High-Level Principles for the

Effective Protection of Whistleblowers)¹, где представлены 12 принципов защиты информаторов, которые разделены на три раздела: создание правовой среды, процедуры защиты информаторов и правоприменительные процедуры. Среди других подобных документов можно выделить Принципы корпоративного управления ОЭСР (G20/OECD Principles of Corporate Governance)², а также Международные принципы в области законодательства об информировании (International Principles for Whistleblower Legislation)³.

Условно данные практики можно разделить на институты, которые государствам рекомендуется внедрить на законодательном уровне, и инструменты локального регулирования, которые каждая компания может имплементировать в свои внутренние документы.

8.3.1. В области создания надлежащей правовой среды для развития корпоративного информаторства государствам рекомендуется:

разработать и принять положения законодательства, в которых будут содержаться механизмы по защите корпоративных информаторов. Такое законодательство, в частности, должно поощрять организации к созданию и внедрению мер защиты информаторов на локальном уровне. При этом желательным является принятие отдельного законодательного акта, посвященного защите информаторов как в публичном, так и в частном секторе.

¹ G20 High-Level Principles for the Effective Protection of Whistleblowers. Полный текст документа доступен по ссылке: https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_07.pdf

² G20/OECD Principles of Corporate Governance. Полный текст документа доступен по ссылке: https://www.oecd.org/en/publications/2023/09/g20-oecd-principles-of-corporate-governance-2023_60836fcb.html

³ International Principles for Whistleblower Legislation. Best Practices for Laws to Protect Whistleblowers and Support Whistleblowing in the Public Interest (Transparency International, 2013). Полный текст документа доступен по ссылке: <https://www.transparency.org/en/publications/international-principles-for-whistleblower-legislation>

Четко определить в законодательстве ситуации, когда информатор будет иметь право на защиту. В частности, законодательство должно содержать конкретный перечень фактов, раскрытие информации о которых будет подлежать защите, а также определять случаи, которые защите не подлежат.

Распространить законодательную защиту на максимально широкий круг потенциальных информаторов. В идеале их круг должен не ограничиваться только работниками, находящимися с организацией в трудовых отношениях, а распространяться на иных стейкхолдеров, в том числе лиц, которые хотят сохранить конфиденциальность. В частности, законодателю не рекомендуется исключать из сферы потенциальной защиты лиц, не являющихся сотрудниками организации (например, контрагентов компании по гражданско-правовым договорам), если их знания о нарушениях столь же полезны и они могут аналогичным образом пострадать от пагубных последствий раскрытия информации о правонарушениях.

8.3.2. В области регулирования корпоративного информаторства на локальном уровне корпорациям рекомендуется:

обеспечить и закрепить в своих внутренних документах разнообразные каналы передачи информации и средства поддержки информаторов. Для облегчения процесса информирования и укрепления доверия к нему со стороны информаторов компаниям важно предусмотреть разнообразные, доступные каналы информирования и распространить защиту на всех лиц, имеющих право сообщать сведения по установленным каналам. Подобные каналы могут быть как внутренними, так и внешними (например, для информирования правоохранительных и иных компетентных органов). К внутренним каналам можно отнести специальное должностное лицо, члена правления или совета директоров (trusted leader), а также горячую линию (как правило, анонимную). Как показывает практика, анонимное информирование способствует тому, что сотрудники

с большей вероятностью будут сообщать о потенциальных или фактических правонарушениях либо обращаться за советом, не опасаясь преследования со стороны руководства.

Внешними каналами в зависимости от характера информации могут быть адвокаты, средства массовой информации, правоохранительные органы или иные государственные структуры. Компания также может прибегнуть к услугам внешних организаций для создания безопасного и анонимного внутреннего канала связи для своих сотрудников. Преимуществом их привлечения является отсутствие конфликта интересов, а также гарантия сохранения анонимности информатора и передачи данных лицам, находящимся на вершине организационной пирамиды.

Наилучшей практикой является создание канала обратной связи на уровне совета директоров, поскольку именно этот орган занимает высшее место в корпоративной иерархии и призван контролировать деятельность менеджмента. В частности, такая рекомендация содержится в Принципах корпоративного управления ОЭСР: согласно ч. 4 (Е) документа, стейкхолдеры должны иметь возможность свободно сообщать совету директоров о незаконных или неэтичных практиках в компании. В связи с этим Принципы корпоративного управления ОЭСР рекомендуют совету директоров не только предоставлять таким лицам конфиденциальный прямой доступ к кому-либо из независимых членов (как правило, члену комитета по аудиту или этике), но и обеспечивать им реальную защиту от возможных санкций со стороны заинтересованных в их молчании должностных лиц.

Компаниям также рекомендуется предусмотреть, чтобы положения заключаемых ими трудовых договоров, в том числе содержащие условия по неразглашению информации или выплате выходных пособий, не мешали работникам сообщать сведения под защитой, не лишали их защиты и не наказывали их за это.

Обеспечить конфиденциальность для информаторов. Внутренние документы компании должны гарантировать конфиденциальность личности информатора

и содержания информационного сообщения. Компаниям также рекомендуется внедрить механизмы и каналы анонимного информирования.

Определить как можно более полный перечень возможных мер репрессивного характера в отношении информаторов, от которых их необходимо защитить. Учитывая, что меры воздействия на информаторов могут принимать различные формы, не ограничиваясь преследованием на рабочем месте, при разработке системы их защиты компаниям рекомендуется определить во внутренних документах максимально полный перечень видов давления на информаторов.

Обеспечивать информаторам надежную и всестороннюю защиту их прав. Компаниям рекомендуется предоставлять информаторам защиту от любых форм преследования или дискриминации, в том числе средства правовой защиты для устранения прямого и косвенного ущерба, причиненного в результате информирования. Помимо этого, рекомендуется информировать сотрудников о существующих в организации каналах обратной связи и о том, как их использовать, а также о средствах защиты, доступных в случае применения к ним любых форм давления.

Предусмотреть санкции в отношении должностных лиц, оказывающих давление на информаторов. Компаниям рекомендуется применять эффективные, соразмерные и сдерживающие санкции в отношении тех руководителей, которые мстят информаторам или оказывают на них давление, независимо от занимаемых ими должностей.

Обеспечить невозможность привлечения к ответственности информаторов в связи с раскрытием защищенной информации. Компаниям рекомендуется предусмотреть во внутренних документах положение, согласно которому информаторы не подвергаются дисциплинарным санкциям и иным формам ответственности на основании подобных сообщений, а также установить санкции для руководителей, применяющих меры репрессивного характера в отношении информаторов и лиц, нарушающих принципы конфиденциальности информирования, независимо от их должности

или положения. При этом компаниям также рекомендуется рассмотреть возможность введения санкций в отношении информаторов, сообщения которых признаны заведомо ложными. При необходимости компании вправе предоставлять компенсацию лицам, понесшим ущерб от ложных сообщений.

Повышать осведомленность информаторов о существующих механизмах их защиты. Компаниям рекомендуется повышать осведомленность информаторов об имеющихся механизмах защиты, в том числе с целью изменения общественного восприятия и отношения к корпоративному информированию. Важно способствовать распространению осведомленности о пользе информирования и его доступных защищенных каналах, а также политике защиты информаторов от санкций и преследований.

Достижение поставленной цели невозможно без создания в компании культуры открытых дверей и транспарентности, когда сотрудники на всех уровнях могут донести до вышестоящего руководства свои опасения. Такая корпоративная культура должна начинаться с уровня председателя совета директоров и заканчиваться уровнем линейных менеджеров (в зарубежной литературе для обозначения подобной системы применяется термин «tone from the top», то есть тон, задаваемый с самого верха). В практическом плане это означает то, что все работники обязаны быть хорошо осведомленными о наличии, формах и процедуре информирования, которая должна быть максимально простой и доступной. В частности, компания может организовать обучение для сотрудников по ряду ключевых аспектов информирования, таких как порядок подачи жалобы и ее рассмотрения, меры защиты от санкций со стороны руководства. Помимо этого, компаниям рекомендуется проводить специализированное обучение лиц, ответственных за прием от работников подобных информационных сообщений, и обеспечить разработку для них четких инструкций.

Осуществлять мониторинг работы системы информирования и оценивать ее эффективность. Компаниям рекомендуется мониторить и в случае

необходимости пересматривать свои механизмы защиты информаторов, в частности регулярно оценивать их эффективность.

В представленных международных документах подчеркивается, что перечисленные принципы и подходы служат руководством для разработки законодательства и локальных нормативных актов. Вместе с тем они должны быть адаптированы к политическим, социальным и культурным особенностям конкретной страны, а также к корпоративной культуре каждой отдельной компании.

* * *

Как уже отмечалось выше, внедрение в законодательство и корпоративную практику системы информаторства и защиты информаторов является непростой задачей. Помимо чисто практических проблем, связанных с противодействием информаторам со стороны менеджмента, корпоративное информаторство является сложным и неоднозначным институтом как в правовом, так и в этическо-нравственном плане. Его внедрение связано с необходимостью государственных органов или руководства корпораций совершать политико-правовой, а зачастую и морально-этический выбор.

С точки зрения права главная проблема состоит в определении: какие именно нарушения и недобросовестные практики должны подпадать под категорию «защищенное информирование». В качестве подобных нарушений в законодательстве зарубежных стран чаще всего называются коррупция, мошенничество, нарушение закона или внутренних документов и процедур компании, угроза интересам компании или общественным интересам, а также неэтичная и аморальная деятельность наделенных властью лиц¹. Однако, если в случае с нарушением закона или локальных нормативных актов двусмысленности не возникает, то категория «угроза интересам компании или общественным интересам» (которая, к примеру, используется

¹ *Schultz D., Harutyunyan K. Combating Corruption: The Development of Whistleblowing Laws in the United States, Europe, and Armenia // International Comparative Jurisprudence. 2015. P. 87.*

в законодательстве Великобритании) является оценочной и создает пространство для неопределенности и дискреции. Аналогичная ситуация возникает в отношении неэтичной и аморальной деятельности должностных лиц – универсальные для всех стандарты морали и этики отсутствуют. В результате возникает ситуация, когда работник, раскрывая информацию о тех или иных недобросовестных практиках, не может быть уверен, будет ли ему предоставлена защита. В конечном счете все может зависеть от дискреционного решения суда или даже от взгляда на проблему того руководителя (trusted leader), к которому обратится сотрудник.

Другая правовая проблема заключается в том, должно ли подлежать защите любое информирование о недобросовестных практиках, не являющееся заведомо ложным, либо защите подлежит только информирование из добросовестных побуждений, а не по мотивам личной неприязни к вышестоящему руководству, мести, корысти, продвижения по службе и т.д. Дискуссия о том, какие мотивы информирования могут рассматриваться в качестве надлежащих, а какие нет, также лежит в морально-этической плоскости и не имеет однозначного ответа. Как уже отмечалось, законодательство США не видит проблемы в информировании из корыстных побуждений и даже финансово поощряет информаторов, в то время как в большинстве европейских стран подобная практика считается неприемлемой. Интересен в этом отношении опыт Великобритании, где в изначальной редакции PIDA содержалось требование к добросовестности информатора, однако впоследствии от данного критерия решено было отказаться из-за сложности доказывания его побудительных мотивов.

Корпоративное информаторство является дискуссионным с точки зрения этики и морали. Сторонники данной практики утверждают, что доносить правду до руководства с целью предотвратить незаконную или вредную для компании деятельность – этически верное и правильное поведение. Вместе с тем их оппоненты рассматривают корпоративное информаторство как проявление нелояльности и нарушение этики взаимоотношений с коллегами. Они утверждают, что мотивом

информирования могут быть не интересы корпорации, а личные мотивы информатора, например его желание отомстить своему начальнику, продвинуться по службе или сделать конфиденциальные сведения достоянием гласности. И напротив, нежелание говорить правду может быть вызвано не нелояльностью или страхом возмездия, а стремлением сохранить добрые отношения с коллегами или руководством компании.

С морально-этической точки зрения корпоративное информаторство воспринимается также неоднозначно – во многих национальных культурах такое поведение рассматривается как доносительство или предательство и подлежит общественному осуждению¹. Этические вопросы возникают в случае, если информатор в соответствии с нормами законодательства (как, например, в США или Канаде) или внутренними документами компании получает за предоставление информации денежное вознаграждение.

Вознаграждение за предоставленные сведения, во-первых, искажает мотивы информирования с моральных на материальные; во-вторых, стимулирует работников информировать руководство компании или государственные органы при любом подходящем случае (даже когда проблему можно решить без их вмешательства), а также получить информацию любой ценой. Представляется, что именно по этой причине вознаграждение информаторов не практикуется в большинстве европейских стран и является не мировым трендом, а скорее уникальной особенностью

¹ К примеру, в России в некоторых случаях термин «whistleblower» переводится как «осведомитель», а понятия «информатор» и «осведомитель» употребляются как синонимы в русскоязычном контексте. Представляется, что такое употребление не вполне обоснованно в связи с тем, что в Российской Федерации и постсоветских странах исторически под осведомителем понимали сотрудника спецслужб и данный термин сопровождался негативной коннотацией (см., например, доклад Transparency International, в котором анализируется культурный и политический контекст употребления термина «whistleblower» в разных странах, в том числе тех, в которых существовали коммунистические режимы: Alternative to Silence: Whistleblower Protection in 10 European Countries, Berlin, 2009 [Электронный ресурс]. URL: <https://www.transparency.org/en/publications/alternative-to-silence-whistleblower-protection-in-10-european-countries>

североамериканской корпоративной культуры¹. В конечном счете ответ на вопрос, почему в одной стране whistleblowing подробно регулируется законодательством и активно функционирует, а в другой – нет, может лежать не только в правовой, но и в социальной, этической или культурной плоскостях.



¹ Как отмечается в упоминавшемся исследовании Freshfields Bruckhaus Deringer, в большинстве европейских юрисдикций сохраняется скептическое отношение к финансовым стимулам для информаторов и пропагандируется иной подход к развитию культуры корпоративного информаторства.