TRANSPARENCY INTERNATIONAL
Korruptsioonivaba Eesti

МЕХАНИЗМ ИНФОРМИРОВАНИЯ НА ПРЕДПРИЯТИИ

ИНСТРУМЕНТАРИЙ

«Эстония без коррупции» (Korruptsioonivaba Eesti, KVE) – это некоммерческая волонтерская организация, целью которой является последовательное предотвращение коррупции, повышение информированности по вопросам коррупции, а также мониторинг и анализ уровня коррупции в обществе Эстонии. KVE является аккредитованным представителем Transparency International в Эстонии.

Автор: Анни Ятса

Составление инструментария профинансировано в рамках проекта «Развитие наилучших механизмов и практик информирования о неправомерном поведении в частном секторе Эстонии». Transparency International не несет ответственности за использование содержащегося в инструментарии материала.

ОГЛАВЛЕНИЕ

АННОТАЦИЯ

О ненадлежащем поведении на предприятии в первую очередь становится известно тем, кто на нем или на него работает. Несмотря на то, что именно эти находящиеся в трудовых отношениях лица имеют самые лучшие возможности, чтобы сообщить о неправомерном поведении еще до того, как предприятию будет причинен ущерб, они часто этого не делают, потому что боятся потерять работу, опасаются мести коллег или не верят, что от того, что они сообщат, что-то изменится.

Эффективный механизм информирования помогает защитить организации от последствий неправомерного поведения, избежать материальных и репутационных потерь. Указанными методами работники могут информировать о ненадлежащем или противозаконном поведении, внося таким образом свой вклад в развитие культуры, бренда, ценностей и рост предприятия.

Принципы механизма информирования:

1. руководство предприятия побуждает работников и партнеров информировать о неправомерном поведении;
2. конфиденциальность и анонимность гарантированы;
3. рассмотрение сообщений эффективно и независимо, а также
4. информаторы защищены от любых преследований.

При создании и внедрении механизма информирования предприятие учитывает:

1. свои ценности и установки работников;
2. вытекающие из закона обязательства;
3. размер организации, а также
4. человеческие и денежные ресурсы.

Организация готова:

1. установить четкие роли и сферы ответственности;
2. собирать исходную информацию как у работников, руководства, так и у третьих лиц;
3. создать и последовательно применять план коммуникации;
4. составить инструкции для тех, кто передает и получает информацию;
5. наладить безопасные и простые в использовании каналы информирования и
6. поддерживать механизм информирования в актуальном состоянии.

Благоприятствование информированию и реализация защиты информаторов принесут предприятию реальную пользу в виде:

1. укрепления ориентированности на честную деятельность и социальную ответственность;
2. предотвращения и смягчения скандалов и репутационного ущерба;
3. предотвращения и уменьшения материального ущерба;
4. последовательного совершенствования управления рисками;
5. повышения культуры предприятия.

ОПРЕДЕЛЕНИЯ

Телефон для справок, или helpline	По телефону для справок работник может получить совет о том, как сообщить о неправомерном поведении и о каких случаях сообщать по горячей линии.
Коррупция	Злоупотребление предоставленными правами в личных целях.
Горячая линия, или телефон доверия, или hotline	По горячей линии можно сообщить о неправомерном поведении.
Информатор	Лицо, сообщающее о неправомерном поведении.
Защита информатора	Меры защиты сообщившего о неправомерном поведении лица в случае преследований, например обеспечение конфиденциальности личности информатора и/или факта сообщения.
Политика информирования, порядок или инструкция по информированию о неправомерном поведении	В политике информирования устанавливается, что именно предприятие считает неправомерным поведением, как предприятие реагирует на нарушение своих ценностных принципов, как можно сообщать о неправомерном поведении, как корректно принимать такое сообщение и как защищать информаторов предприятия от преследований.
Неправомерное поведение, или ненадлежащее деяние	Действие, которое идет вразрез с ценностями предприятия и законами.
Преследование	Притеснение, дискриминация, увольнение и тому подобные действия в отношении лица, сообщившего о неправомерном поведении.

ВВЕДЕНИЕ

Складывается впечатление, что общество в Эстонии становится всё более прозрачным и этичным. Это отражается в ежегодном международном индексе восприятия коррупции (CPI), согласно которому в 2018 году Эстония с 73 пунктами занимала 18-е место в мире и входила в число стран с наиболее низким данным показателем. В 2012 году Эстонии набрала 64 пункта и занимала лишь 32-е место.

К сожалению, CPI не учитывает частный сектор, хотя ясно, что именно частный сектор Эстонии в годы после восстановления независимости предпринял заметные шаги в направлении развития честного бизнеса, а бизнес-культуру в нем можно сравнить, скорее, с финской и шведской, которые занимают верхние позиции в CPI, чем с другими странами Восточной Европы.

Концепция бизнес-коррупции еще только вырисовывается, поскольку среди предпринимателей распространены неверные представления, позволяющие многим незаконным практикам, таким как откаты, заключение договоров при конфликте интересов и т.п., оставаться частью деловой жизни. В предотвращении и выявлении случаев коррупции информаторы играют большую роль, однако информирование о неправомерном поведении в частном секторе обычно не находит широкого резонанса в обществе. С одной стороны, вероятно, о неправомерном поведении в частном секторе сообщается реже, поскольку мер по защите работников в нем принимается меньше, чем в госсекторе. С другой стороны, выявленные случаи зачастую улаживаются внутри предприятия, чтобы общественность о них не узнала.

Исключениями являются случаи отмывания денег на международном уровне, угроза окружающей среде и нарушения прав человека. Во время составления инструментария в Эстонии велось расследование отмывания денег через эстонский филиал Danske Bank, о котором внутри банка и Финансовой инспекции сообщил работник банка Говард Уилкинсон. Тот факт, что личность информатора стала известна общественности, явно свидетельствует о том, что механизм информирования не сработал и конфиденциальность информатора обеспечить не удалось.

Одним из первых наиболее известных информаторов в частном секторе был Стенли Адамс, который, занимая пост руководителя швейцарской фармацевтической компании Hoffmann-LaRoche, обнаружил, что предприятие участвует в антиконкурентном сговоре по ценам на витамины. Соответствующие документы он передал в Европейское экономическое сообщество, однако в ходе расследования его имя всплыло, и Адамс сам был признан виновным в промышленном шпионаже. Значительная часть хороших законов по защите информаторов принимается именно для предотвращения таких ситуаций – чтобы информатору достаточно было только сообщить о своих подозрениях, а сбором доказательств занимались бы уже те, кому положено.

Нередки и случаи, когда информатора дискредитируют с целью переключить внимание с проблемы на личность. Информатору угрожает коллективная дискриминация и преследования, потеря работы и другие негативные последствия. Предприятие, которое ценит честность в бизнесе, свою добрую репутацию среди клиентов и партнеров, а также надлежащее использование ресурсов, защищает работников, сообщающих в интересах предприятия о неправомерном поведении. Эффективный механизм информирования помогает предприятию заранее узнать о проблемах и защитить своего работника.

Рассматриваемого рода информирование в английском языке обозначается термином «whistleblowing», т. е. «свист в свисток», что указывает на своеобразные параллели,

например со спортивным судейством или полицией, когда пытаются указать на ошибку или опасность. С середины XX века существительным от этого английского слова называют людей, которые сообщают о противоправных действиях в организации.[1] Так информаторы получили в англоязычной культуре, скорее, позитивную коннотацию.

В эстонском языке нет адекватного соответствия термину «whistleblower», кроме слова «vihjeandja», переведенном здесь на русский как «информатор». Используются также термины «väärkäitumisest teavitaja», «vääritust teost teavitaja» и «vilepuhuja», переведенные здесь на русский соответственно «информатор о неправомерном поведении», «информатор о ненадлежащем поведении» и «информатор». Последний термин по-эстонски – калька с английского («свистун в свисток») и, вероятно, не приживется. Институт эстонского языка рекомендовал в качестве альтернативы «vilemees», «informeerija» и «vihjaja».[2] Что приживется – покажет время. В настоящем пособии используются только эстонские термины «vihjeandja» и «väärkäitumisest teavitaja», переведенные на русский язык как «информатор» и «информатор о неправомерном поведении».

В культурном пространстве Эстонии к информаторам долгое время относились негативно по историческим причинам. До сих пор их иногда обзывают «стукачами», «жалобщиками» и другими обидными словами из советского лексикона, считая, скорее, предателями, чем защитниками общественных интересов.

Истоки этого кроются в культурной истории, испытавшей влияние присущего католичеству и православию жесткого социального контроля, при котором инакомыслящих, особенно реформаторов, клеймили и изгоняли из общества. Православие повлияло также на распространившуюся в России конца XIX – начала XX века мощную воровскую субкультуру, в которой любой донос и сотрудничество с властями жестоко наказывались. Советская власть умело использовала социальные методы воздействия, благодаря чему любое инакомыслие политизировалось. Такая стигматизация породила коррумпированную культуру, когда находящиеся на самых разных уровнях власти люди всеми возможными способами старались извлечь выгоду и за счет государства, и за счет работодателя.

В течение долгого времени формировалось представление о государстве и работодателях как об угнетателях, которым нужно во что бы то ни стало противостоять, и при этом «своих», т. е. других недовольных, «не сдавать». Информаторы автоматически считались «предателями», и такому пониманию сами способствовали и те, кто был нечист на руку. Благодаря систематическому изменению установок, стал изменяться и этот стереотип. Значительная роль в этом принадлежит более широкому привлечению людей к управлению предприятиями и масштабной просветительской работе, охватывающей как этические, так и экономические аспекты управления. Информирование превращается в систему раннего оповещения, которая помогает снижать риски и способствует оздоровлению микроклимата в организации.

Информирование о неправомерном поведении – один из наиболее эффективных способов выявления коррупции. Проведенное в 2018 году Ассоциацией сертифицированных специалистов по борьбе с мошенничеством (ACFE) исследование показало, что информирование является преобладающим путем раскрытия мошенничества, составляя 40% всех случаев. За информированием всего с 15% следует внутренний аудит.

Бытующие внутри организации неверные представления об информировании, неразвитые его механизмы и дурной пример со стороны руководства, выражающийся, например, в неспособности защитить своих работников от преследований, препятствуют его развитию.

[1] Подробнее о дефиниции понятия «информирование» можно узнать из защищенной в 2007 году Аннели Сихвер магистерской работы «Teavitaja kaitse («Vilepuhuja kaitse») süsteemi rakendatavus korruptsiooni avalikustamisel Eesti avalikus teenistuses».

[2] Термин «Vilepuhuja» с лингвистической точки зрения рассмотрен Майре Раадик в номере газеты Postimees от 14.06.2016, в рубрике EKI keelekool: https://arvamus.postimees.ee/3690159/eki-keelekool-koneisik-ja-vilepuhuja.

Для того чтобы с помощью настоящего инструментария предотвращать на своем предприятии коррупцию и неправомерное поведение, руководство должно позаботиться о том, чтобы в организации на каждом ее уровне была принята нулевая толерантность к коррупции, предлагать работникам поддержку в их следовании своим убеждениям, защищать работников от преследований. Целью защиты информирования является побуждение информаторов к тому, чтобы они сообщали о коррупции и другом неправомерном поведении.

Какой бы ни была организация, крупной или малой, продвижение в культуре труда открытости способствует проявлению множества полезных факторов.

Поддерживая информирование о неправомерном поведении, предприятие сможет лучше:

1. предотвращать неправомерное поведение;
2. заранее выявлять проблемы;
3. обеспечивать, чтобы критически важные сообщения доходили до людей, которые могут решить проблему;
4. демонстрировать акционерам, госучреждениям и общественности, что предприятие в состоянии брать на себя ответственность и хорошо справляется;
5. бороться с анонимными и злонамеренными утечками в СМИ;
6. предотвращать несчастные случаи, избегать судебных разбирательств и инспекций с вытекающими из них расходами и компенсациями;
7. выступать как серьезный и надежный партнер;
8. поддерживать и улучшать свое реноме.

Если вы считаете, что эти цели являются для вашей организации первоочередными, то этот инструментарий предназначен именно для вас.

Инструментарий информирования о неправомерном поведении – лишь часть мер по профилактике коррупции, которые, в зависимости от размера, ресурсов и мотивации предприятия, могут включать в себя и другие методы, способствующие честному ведению бизнеса. Для начала можно провести предназначенные для руководителей государственных коммерческих объединений электронные обучающие курсы, которые помогут и руководителям частного сектора в приобретении знаний по предотвращению коррупции и помогут кое-что исправить у себя на предприятии.[3]

Для создания безопасных условий информирования существуют разные инструменты, об эффективности и механизме работы которых мы расскажем. При этом мы дадим рекомендации по поводу того, какие инструменты использовать в типовых ситуациях, а какие отставить в сторону и почему.

Инструментарий содержит образцы документов и технических решений, используемых предприятиями в целях рассматриваемого информирования, а также рамочный механизм, который поможет предприятиям наладить у себя простую систему такого информирования.

О составлении инструментария

Автор Анни Ятса занимается вопросами защиты информаторов с 2013 года, когда в Эстонии впервые появилась возможность интервьюировать информаторов и сравнивать их положение здесь с положением информаторов в других восточноевропейских странах. Управление проектами по защите информаторов и их интересов были частью ее повседневной работы в организации «Эстония без коррупции» в качестве руководителя проекта и исполнительного

[3] Электронные курсы: https://www.korruptsioon.ee/sites/www.korruptsioon.ee/avalike-ettevotete-korruptsiooniennetus-2016/#sections.

директора до 2018 года. Она бакалавр скандинавистики и политологии, магистр госуправления.

Настоящее пособие составлено в период с августа 2018-го по апрель 2019 года. Инструментарий основан на передовом опыте Transparency International и других международных организаций, занимающихся этой темой. Историю информирования помог описать культуролог и член организации Тынис Мутть. При написании раздела о защите данных учитывались указания Инспекции по защите данных. Словом и делом помогла также исполнительный директор объединения «Эстония без коррупции» Карина Паю.

Жизненными примерами и советами поделились руководители и участники четырех организованных объединением мастер-классов.

ЧТО ТАКОЕ МЕХАНИЗМ ИНФОРМИРОВАНИЯ?

Механизм информирования, или система мер информирования о неправомерном поведении, состоит из политик, т. е. инструкций и процедур, побуждающих работников, а также третьи стороны, в частности поставщиков и клиентов, сообщать о неправомерном поведении на предприятии.

Под неправомерным поведением понимается в основном требование, предложение и передача взятки, мошенничество, причинение ущерба окружающей среде, нарушение правил гигиены труда, дискриминация, притеснения, решения, принятые при конфликте интересов, а также присвоение имущества предприятия.

Людей, сообщивших о неправомерном поведении, от преследований защищают аффективные механизмы, которые должны также указывать на возможности предотвращения или уменьшения ущерба, причиняемого неправомерным поведением третьим лицам и самому предприятию.

РЕКОМЕНДАЦИЯ

Transparency International: ПРИНЦИПЫ ХОРОШЕГО МЕХАНИЗМА ИНФОРМИРОВАНИЯ

1. Руководство побуждает работников и партнеров информировать о неправомерном поведении.
2. Конфиденциальность и анонимность гарантированы.
3. Рассмотрение сообщений эффективно и независимо.
4. Информаторы надежно и прозрачно защищены от любых преследований.

ПОЧЕМУ ПРЕДПРИЯТИЯ ПОДДЕРЖИВАЮТ ИНФОРМИРОВАНИЕ?

Согласно существующим оценкам, прибыль предприятия оказывается на 5% больше, если коррупционных расходов, например в связи со взятками, откатами и хищениями, нет.[4] Механизмы информирования работают во благо коммерческих интересов, защищая предприятие от ущерба, связанного с неправомерным поведением, в т. ч. от ущерба материального и репутационного. Эффективные механизмы информирования на предприятии развивают внутри него культуру доверия, поддерживают бренд, формируют и продвигают ценности.

В мировых СМИ всё чаще говорится о том, к каким катастрофическим последствиям приводит несоблюдение закона и этических норм, – это травмы, смерти, ущерб окружающей среде и нарушение прав человека. Налаженные внутри предприятия эффективные механизмы рассматриваемого информирования, культура доверия и быстрая реакция руководства могли бы помочь избежать последствий и ущерба для бизнеса или смягчить их.

[4] Report to the Nations on Occupational Fraud and Abuse (2016) Association of Certified Fraud Examiners.

Предприятие заинтересовано в том, чтобы как можно раньше узнавать о проблемах, однако ясно, что руководство не в состоянии само за всем следить. О неправомерном поведении сообщают в первую очередь сознательные работники. Именно они располагают наилучшими возможностями информирования еще до того, как предприятию причинен ущерб. К сожалению, многие этого не делают, если система информирования о неправомерном поведении на предприятии кажется им запутанной, неработоспособной или они ей не доверяют.

ПРИМЕР

В 2015 году газета Eesti Päevaleht[5] написала о том, что повар кейтеринговой компании, обслуживающий сауэский детский сад Midrimaa привлек внимание заведующей детским садом и вице-мэра к тому, что компания экономит и дети получают еды меньше, чем полагается. Взятые Департаментом здоровья анализы подтвердили, что питательных веществ в детской еде было всего 53% от необходимого количества.

Повара уволили.

Из этого случая можно сделать два вывода:

1. Вместо того, чтобы выслушать работника, похвалить его и заняться проблемой, его уволили. Культура предприятия не поощряла открытое общение, предприятие не придерживалось принципов честного ведения бизнеса.

2. Мало того, что с увольнением работника проблема не рассосалась, она получила огласку через крупную ежедневную газету. Репутационный ущерб устойчив, потому что поисковые системы помнят всё, а подобные статьи[6], в которых родители переживают о том, не морят ли голодом их детей, продолжают выходить. При налаживании связей с новыми партнерами всегда может получиться, что предприятию придется оправдываться за старое. Вытекающий из репутационного материальный ущерб не поддается оценке, и он определенно не исключен.

Простой механизм информирования, который можно было бы запустить, назначив доверенное лицо, позволил бы нормальным образом и без увольнений решить описанную проблему.

Но при всем при этом следует помнить, что если предприятие сознательно нарушает договорные обязательства, то речь идет о проблеме другого рода, для решения которой на предприятии нужно изменить культуру управления.

[5] Подробнее: http://epl.delfi.ee/news/eesti/toitlustusfirma-vallandas-saue-lasteaia-koka-kes-probleemide-ule-kaebas?id=71227071.

[6] Подробнее: https://www.err.ee/694131/tallinna-linn-dussmanni-pakutaval-lasteaiatoidul-probleeme-ei-nae.

ЭЛЕМЕНТЫ ЭФФЕКТИВНОГО МЕХАНИЗМА ИНФОРМИРОВАНИЯ

КОНТРОЛЬНЫЙ СПИСОК ПРОЦЕССА СОЗДАНИЯ И ВНЕДРЕНИЯ МЕХАНИЗМА

В упрощенном виде внедрение механизма информирования состоит из пяти этапов, элементы которого подробно описываются в инструментарии. Контрольный список поможет предприятию шаг за шагом разработать подходящий для себя механизм, избегая принятия несоответствующих мер и разбазаривания ресурсов.

Этап	Цель	Инструмент	✓
I. Оценка необходимости	Меры должны прижиться в организации	Анализ степени зрелости организации	
		Анализ ресурсов организации	
		Опрос работников	
		Анализ законодательных требований	
		Внешние оценки, аудиты	

Прежде всего организация оценивает:

1. установлены ли на предприятии ценности;
2. каково отношение и опыт работников в связи с информированием;
3. является ли внедрение мер информирования рекомендацией какой-либо третьей стороны, вытекающей из нормативного регулирования обязанностью или внутренней инициативой предприятия.

II. Получение поддержки	Для внедрения мер достаточно ресурсов	Представление руководству на утверждение	

Инициатива по внедрению новых мер не всегда должна исходить от начальства. В таком случае руководителей следует убедить и объяснить им, в чем выигрыш предприятия от введения мер информирования.

Этап	Цель	Инструмент	✓
III. Организация мер	Четкие зоны ответственности	Распределение ролей, в т. ч. назначение ответственного	
	Формирование чувства хозяина	Получение исходных данных от руководства и коллектива	
		Утверждение мер	

В интересах организации – не допускать нечетко очерченных ролей и зон ответственности, поэтому, для того чтобы меры оказались действенными, наряду с поддержкой руководства, крайне важно и назначение конкретного ответственного лица или отдела.

Лица, которые отвечают за механизм информирования, заботятся о выработке и внедрении мер.

IV. Внедрение мер	Каждая мера имеет свою цель	План коммуникации, в т. ч. выступления, напоминания, обучающие занятия	
		Инструкции по информированию для информаторов, руководителей	
		Каналы информирования	
		Обеспечение конфиденциальности	

О мерах работникам следует напоминать при любом удобном случае. Утвержденный план коммуникации, обучающие занятия и повышение общей осведомленности помогают внедрению мер.

Ответственный отдел налаживает в организации надлежащие каналы коммуникации.

Составляются инструкции для руководителей, работников и, если требуется, для третьих лиц. Таким образом обеспечивается, чтобы введение механизма информирования понималось однозначно, а меры принимались корректно.

V. Дополнение мер	Меры должны быть актуальными	Механизм должен проходить регулярную переоценку	
		Регистр сообщений	
		Анализ сообщений	

Этап	Цель	Инструмент	✓

Принятие мер предполагает последовательность и соблюдение установленных процедур, чтобы у работников сохранялось доверие к механизму, без чего о неправомерном поведении сообщать не будут.

По применению мер полезно собирать статистику, чтобы у руководства был обзор ситуации.

Регулярно следует переоценивать актуальность мер и при необходимости их дополнять.

КОНТРОЛЬНЫЙ СПИСОК ДЛЯ ИНСТРУКЦИИ ПО ИНФОРМИРОВАНИЮ

Контрольный список помогает продумать необходимые для безопасного информирования шаги и составить инструкцию о порядке информирования о неправомерном поведении.

Раздел инструкции	Поясняет...	Варианты	Пригодится...	✓
I. Введение	Зачем нашей организации эта инструкция?		Анализ потребностей организации Ценности организации Опрос работников	
	Каким образом инструкция соответствует нашим ценностям?			
II. Информатор	Кто может информировать?	Работники, члены правления, совета	Анализ ресурсов организации	
		Практиканты, волонтеры		
		Партнеры		
		Клиенты, общественность		
III. Неправомерное поведение	О чем ожидаются сообщения?	Поведение, причиняющее ущерб интересам предприятия, например хищение, взятка и т. п.	Законодательство Ценности организации Правила организации труда	
		Жалоба в связи с работой, например на дискриминацию, преследования и т. п.		
IV. Информирование	Как можно сообщить о неправомерном поведении?	Политика открытых дверей		
		Инструкция по информированию		

Раздел инструкции	Поясняет...	Варианты	Пригодится...	✓
	Какие каналы можно использовать для информирования?	Горячая линия	Анализ ресурсов организации или ценовые предложения от поставщиков услуг	
		Электронная почта		
		Интернет-анкета		
		Почтовый ящик		
		Социальные сети		
	Каким образом защищен информатор?	Анонимность, конфиденциальность	Обзор обработки данных Ценности организации	
V. Прием сообщений	Кто принимает сообщения?	Непосредственный начальник	Анализ ресурсов организации	
		Доверенное лицо		
		Внутренний аудит или т. п.		
	Что происходит с сообщением дальше?		Схема движения сообщения	
	Как обрабатываются данные?		Анализ обоснованного интереса	
	Контактные данные			

БАЗОВАЯ ИНФОРМАЦИЯ К РАЗМЫШЛЕНИЮ

В 1777 году два офицера американского Континентального флота Ричард Марвен и Сэмюэл Шоу стали свидетелями того, как командующий будущих ВМС США Эзек Хопкинс пытал британских военнопленных. В 1778 году Конгресс США принял первый в мире закон о защите информаторов.

Информирование о неправомерном поведении в законодательстве Эстонии

Эстонские законы не устанавливают для частных предприятий обязательств по созданию механизма рассматриваемого информирования и, таким образом, не предлагают защиты информаторам о неправомерном поведении. Если предприятие хочет, чтобы в случае подозрений работники обращались не в прессу, а к руководству или какому-либо доверенному лицу, нужно сделать больше того, чем требуется законодательством. Порицание недостойного поведения и поощрение честного ведения дел требует от предприятия инициативы и ресурсов, но в любом случае эти усилия помогают защитить бизнес и репутацию, а при случаях коррупции – смягчить связанные с ней последствия.

Эстонское законодательство регулирует рассматриваемое информирование косвенно. Например, принцип равного обращения в трудовых отношениях защищен ст. 3 **Закона о трудовом договоре** (TS) и ст. 13 **Закона о публичной службе** (ATS). Если лицо сообщает о нарушении, его нельзя дискриминировать на рабочем месте или уволить. К сожалению, сложно доказать связь между дискриминацией и информированием, например в случае, если позже лицо остается без повышения. При этом TS не действует в отношении членов правления. Таким образом, формальную защиту закон предлагает, однако ее эффективность сомнительна.

Наиболее конкретно информированием занимается **Закон о противодействии коррупции** (KVS), статья 6 которого требует обеспечения конфиденциальности факта информирования и распределяет бремя доказывания. Чтобы была обеспечена конфиденциальность, случай должен быть квалифицирован как коррупционный[7]. В то же время за нарушение конфиденциальности не предусмотрено никаких санкций, поэтому здесь закон не обеспечивает информатору чувства защищенности.

Безусловно важной в контексте информирования **является защита коммерческой тайны,** которая регулируется директивой ЕС 2016/943, а также Законом о противодействии недобросовестной конкуренции и защите коммерческой тайны. Часть 6 статьи 5 этого закона гласит:

> *Получение, использование или разглашение коммерческой тайны не считается незаконным, если оно необходимо, чтобы:*
> 1. *обнародовать незаконное деяние в целях защиты общественных интересов;*
> 2. *работник мог защитить свои права и интересы через представителя работников, при условии, что разглашение им коммерческой тайны представителю необходимо для исполнения последним своих обязанностей, или*
> 3. *защитить признанные законными интересы.*

К сожалению, директива не регулирует того, что произойдет в случае, если нарушения, о котором сообщили, на самом деле нет или не было. В преамбуле поясняется, что в таком случае следует принять в расчет, что сообщение было сделано из добрых побуждений, однако преамбула не является обязательной к исполнению и, таким образом, невозможно

[7] Какие случаи являются коррупционными, описывается в ст. 3 KVS.

обеспечить, чтобы всех информаторов считали добросовестными. Поскольку речь идет о свежем законе, нужно будет дождаться судебной практики, чтобы механизм его действия прояснился.

Защита источников информации для журналистов[8] вытекает из ч. 1 ст. 73 Уголовно-процессуального кодекса и ст. 15 Закона об услугах средств массовой информации.

ПРИМЕР

РАЗОБЛАЧЕНИЕ ЖУРНАЛИСТСКОГО ИСТОЧНИКА

В 2015 году газета Eesti Päevaleht, насколько известно, впервые задействовала принятый в 2010 году закон, когда вышли статьи о сомнительных обстоятельствах распределения муниципальных квартир в Пыхья-Таллинне.[9]

В гражданской авиации информирование регулируется регламентом 376/2014 Европейского парламента и совета, ст. 47 Закона об авиации и принципом справедливого обращения.

Финансовые учреждения должны обращать внимание на регламент о злоупотреблениях на рынке 596/2014/ЕС, Закон о финансовой инспекции, а также на Закон о рынке ценных бумаг. Отдельные требования вытекают из Закона о противодействии отмыванию денег и финансированию терроризма, которые регулируют обязательство по информированию, конфиденциальность сообщения и освобождение от ответственности, а также систему мер защиты, в т. ч. обязательство по созданию механизма информирования.

ПРИМЕР

РАСКРЫТИЕ ЛИЧНОСТИ ИНФОРМАТОРА В ФИНАНСОВОМ СЕКТОРЕ

Разразившийся в 2018 году скандал с отмыванием денег в Danske Bank, когда через его эстонский филиал было прокачано около 200 миллиардов евро сомнительного происхождения, свидетельствует об отсутствии эффективной защиты информаторов. Имя информатора было опубликовано в СМИ, поскольку то ли сам банк, то ли следственные органы не сумели обеспечить конфиденциальность.[10]

Защита данных

Механизм информирования позволяет работникам безопасно сообщать о случаях мошенничества, коррупции или о другом неправомерном деянии. При этом неизбежна

[8] О защите источников см. в обзоре советника Министерства юстиции Сандры Микли: https://www.just.ee/sites/www.just.ee/files/sandra_mikli._kes_voi_mis_on_allikas_ja_miks_me_teda_kaitseme.pdf

[9] Подробнее в статье Eesti Päevaleht: https://epl.delfi.ee/news/eesti/linnaosavalitsus-uritab-ajakirjaniku-allikat-paljastada?id=73114165

[10] Подробнее – в статье Eesti Ekspress: https://ekspress.delfi.ee/kuum/rehe-papp-danske-skandaali-kaivitas-rahulolematu-tootaja?id=83768509

обработка персональных данных. Так, сообщение обычно касается как подозреваемых в неправомерных деяниях лиц, так и информаторов, а также других свидетелей, их данные собираются, регистрируются, хранятся, раскрываются и уничтожаются.

Действующие в Эстонии организации обязаны соблюдать требования законов Европейского союза, касающихся защиты данных, важнейший из которых – вступивший в силу в мае 2018 года Общий регламент по защите данных (General Data Protection Regulation – GDPR).

РЕКОМЕНДАЦИЯ

Надзором за защитой персональных данных занимается Инспекция по защите данных (AKI).[11]

Кроме надзорных мероприятий, AKI занимается разъяснительной и информационной деятельностью. Инспекция составила множество инструкций и предоставляет всем возможность обращаться к своему дежурному сотруднику с общими вопросами по защите персональных данных. Консультационный телефон инспекции 5620 2341 работает по будням с 10 ч. до 12 ч. и с 14 ч. до 16 ч., по четвергам – с 10 ч. до 12 ч. и с 14 ч. до 15 ч.

Если вопрос более специфический, лучше обратиться письменно по почтовому или электронному адресу: Tatari 39, 10134 Tallinn или info@aki.ee.

В контексте защиты данных создание рассматриваемого механизма информирования допускается только в случае, если это необходимо для исполнения вытекающих из закона обязательств или если у предприятия имеется по этому поводу обоснованный интерес.

Обязательство по созданию предусмотренного законом механизма информирования лежит в Эстонии на кредитных учреждениях, и им проще всего обосновать связанную с поступающими сообщениями обработку персональных данных. Другие организации должны оценить, возможна ли именно у них обработка персональных данных в связи с поступающими по причине обоснованного интереса сообщениями.

Обязательство члена правления коммерческого объединения по должной добросовестности (due diligence) означает, что он должен действовать честно (bona fides) и в интересах организации, иметь достаточно информации при принятии решений и не подвергать ее необоснованным рискам. Крупные международные организации, такие как ЕС и ОЭСР, признают важность следования принципу эффективного управления (good governance) для обеспечения их надлежащего функционирования. Подчеркивается, что выработка подходящих мер, которые позволяли бы правлению или проверяющей комиссии узнавать о нарушениях или сомнительных бухгалтерских либо аудиторских методах, – в интересах каждый организации.

Поскольку вытекающего из закона обязательства у значительной части организаций не имеется, целесообразно провести на предприятии правовой анализ, который позволил бы описать обоснованные интересы при обработке поступающих от персонала сообщений. Иными словами, организация должна оценить, перевешивают ли обоснованные интересы работодателя в управлении угрожающими предприятию или связанным с ним сторонам рисками и в снижении этих рисков – неприкосновенность частной жизни работника в

[11] С принципами работы AKI можно ознакомиться на ее сайте по адресу aki.ee.

результате внедрения механизмов информирования. В результате оценки обоснованного интереса может также оказаться, что на некоторых предприятиях использование механизма информирования невозможно.

РЕКОМЕНДАЦИЯ

Анализ реальных ситуаций позволяет лучше уяснить, имеется ли у организации обоснованный интерес в обработке данных.

При рассмотрении обоснованного интереса следует по возможности учесть и уже имевшие место на предприятии случаи информирования, когда в силу отсутствия соответствующего механизма неправомерное поведение осталось не раскрытым, или когда работник поставил в известность какое-либо третье лицо, например полицию или журналистов.

Статьи 12–14 Общего регламента ЕС по защите данных обязывают каждого ответственного обработчика данных составить и опубликовать документ об условиях защиты персональных данных, т. е. политику конфиденциальности, а статья 30 предписывает составить внутренний обзор по обработке данных на предприятии, который в интересах прозрачности также может быть частично опубликован. Оба документа лучше подготавливать одновременно, поскольку в них присутствует ряд текстуальных совпадений.

В рамках политики конфиденциальности стоит объяснить, как предприятие обрабатывает персональные данные в случае сообщения о неправомерном поведении.[12]

ИНСТРУМЕНТ

УСЛОВИЯ ЗАЩИТЫ ДАННЫХ, ИЛИ ПОЛИТИКА КОНФИДЕНЦИАЛЬНОСТИ[13]

Статьи 12–14 Общего регламента ЕС по защите данных требуют, чтобы организации письменно, в т. ч. в электронном виде, задокументировали условия защиты данных. В документе должно содержаться следующее:

- Название и контактные данные ответственного обработчика (организации), а также имена, фамилии и контактные данные специалиста по защите данных (если назначен)
- Цель
    - Какова цель обработки данных?
        - в т. ч. в контексте рассматриваемого здесь информирования, например выявление и предотвращение мошенничества
    - Каковы правовые основания для обработки данных?
        - в т. ч. оценка обоснованного интереса

[12] Требования к обработке персональных данных подробно рассмотрены в составленной AKI общей инструкции, доступной на сайте инспекции по адресу aki.ee.

[13] Подробнее о том, какие сведения обработчик данных должен раскрывать лицу, данные которого обрабатываются, описано на стр. 43–44 общей инструкции AKI для обработчика персональных данных.

- Процессы
    - Описать, что происходит с персональными данными с момента получения сообщения до прекращения рассмотрения случая:
        - Какие персональные данные собираются?
        - О ком собираются данные?
        - Как данные хранятся?
        - Как долго хранятся данные?
        - Кто имеет доступ к данным?
        - Какие приняты (технические) меры для защиты данных (например, требование конфиденциальности, использование псевдонимов, шифрование и т.п.)?
        - Чьи данные раскрываются и передаются?
        - Каковы права работника (например, требовать ознакомления со своими данными, их исправления, дополнения и т.п.)?

РЕКОМЕНДАЦИЯ

Если каналы информирования открыты и для третьих сторон, например для клиентов, вышеуказанную политику конфиденциальности следует сделать доступной и для них.

Дайте в политике конфиденциальности ссылку на контактные данные каналов информирования (например, номер автоответчика, адрес электронной почты, интернет-формы).

В Эстонии пока нет конкретных инструкций и практики в отношении защиты данных в связи с рассматриваемым в настоящем документе информированием. AKI составила общую инструкцию по Общему регламенту ЕС и трудовым отношениям[14], где защита данных в связи с информированием о неправомерном поведении рассматривается вкратце. В любом случае предприятие должно быть всегда готово разъяснить работникам свой обоснованный интерес в отношении обработки их персональных данных. Еще при разработке механизма предприятия обязаны задуматься о том, почему, какие персональные данные будут обрабатываться и как. Процессы, связанные с информированием, должны быть описаны, продуманы и исходить из обоснованного интереса и необходимости.

[14] Подробнее с инструкцией можно ознакомиться на сайте AKI по адресу aki.ee.

СЛЕДУЕТ УЧЕСТЬ

Подписываясь под правилами внутреннего распорядка на рабочем месте, работник дает согласие на обработку своих данных.

Учитывайте, что согласие можно всегда отозвать, поэтому обеспечьте, чтобы у организации имелся обоснованный интерес для обработки персональных данных с целью информирования и анализ такого интереса был задокументирован.

Ведущие роли

В идеале корпоративная культура должна быть открытой и этичной, поддерживать честную деловую практику, а работники не должны бояться говорить о своих проблемах. В реальности люди не приемлют информирование о неправомерном поведении и тайное осведомительство, однако поддержка информаторов – в интересах предприятия.

Поддержка, которую оказывает **руководство** механизму информирования и честной бизнес-практике, в целом является основой развития культуры предприятия. Поддержка может выражаться как в виде адресованных работникам сообщений, так и посредством мер по повышению осведомленности.

Механизмы информирования наиболее эффективны на тех предприятиях, руководство которых понимает их преимущество и при этом учитывает действующие на предприятии соответствующие инструкции.

ИНСТРУМЕНТ

ПОЛУЧЕНИЕ ОДОБРЕНИЯ РУКОВОДСТВА

Если руководство не уверено в необходимости механизма информирования или тема только появилась на повестке дня, следует прояснить:

1. Почему эти меры следует внедрить на предприятии.
2. На что эти меры направлены.
3. Чего потребует внедрение мер от предприятия.
4. Чего потребует внедрение мер от правления/совета.

Используйте реакцию руководства в качестве исходных данных при разработке механизма.

Руководство активно поддерживает информирование внутри предприятия, обеспечивая, чтобы:

1. сообщения корректно принимались;
2. сообщения тщательно изучались;
3. информатору при необходимости была предоставлена поддержка и защита.

Следование этим принципам побудит других потенциальных информаторов делиться своими сомнениями.

Для того чтобы механизм информирования работал, руководству следует найти конкретного человека или отдел, который этот механизм возглавит.

ИНСТРУМЕНТ

РАСПРЕДЕЛЕНИЕ РОЛЕЙ

1. Назначьте конкретного человека или отдел для разработки и внедрения механизма.

2. Обеспечьте, чтобы у них было достаточно ресурсов, т. е. денег, инструментов, людей и времени.

3. Обеспечьте, чтобы работники были в курсе назначения ответственного лица и используйте возможности для повышения осведомленности персонала по вопросам информирования.

4. Регулярно требуйте обратной связи, чтобы при необходимости поддержать ответственных лиц дополнительными ресурсами или, например, заявлениями.

СЛЕДУЕТ УЧЕСТЬ

Неясные роли и сферы ответственности препятствуют разработке и внедрению мер.

ИНСТРУМЕНТ

ВОВЛЕЧЕНИЕ КОЛЛЕКТИВА

Получение необходимых исходных данных для разработки мер:

1. Поинтересуйтесь у коллектива мнениями по поводу инструкции и мер. Это поможет формированию чувства собственника, а также подчеркнет, что все действуют сообща и с благими намерениями.

2. Всегда устанавливайте сроки.

3. Если широкого обсуждения при формировании политики информирования не получится – не беспокойтесь. Это деликатная тема, но есть основания полагать, что с предложенными материалами люди ознакомятся. В таком случае имеет смысл побеседовать с менеджерами, чтобы все поняли, для чего эти меры нужны.

Для получения исходных данных можно воспользоваться, например, таким инструментом, как

Опрос об осведомленности работников по информированию о неправомерном поведении.

Затраты

Несмотря на то, что создание и поддержка механизма информирования обычно слишком затратными не считаются, тем не менее, стоит обратить внимание на некоторые связанные с конкретными мероприятиями расходы – на презентацию механизма и управление им, на расследование сообщений и обратную связь, а также на обучение. Это позволит гарантировать, что эффективность механизма не пострадает от нехватки ресурсов.

При разработке механизма рекомендуется учитывать также расходы на вовлечение, подразумевающее консультации с работниками, руководством и другими важными сторонами, чтобы создаваемый механизм соответствовал потребностям компании. Кроме того, такие предварительные консультации позволят лучше понять, учтены ли в бюджете все расходы, необходимые для разработки и поддержания механизма. В зависимости от культуры компании может, например, отпасть необходимость в написании отдельной инструкции, достаточно будет рассмотрения соответствующих вопросов в каком-либо другом документе.

Размер и ресурсы компании

Механизм информирования, который подходит для одной компании, может не подойти для другой. Механизм должен быть адекватен размерам и рисковому профилю.

На малых и средних предприятиях (VKE) рассматриваемые механизмы распространены мало.[15] Поскольку у VKE нет характерных для крупных организаций структур и ресурсов, при выстраивании системы информировании о неправомерном поведении здесь учитываются специфические потребности и ограничения.

Если малым предприятием руководит человек, который поименно знает всех работников, то отдельной инструкции по информированию, как правило, не требуется – достаточно только проводить политику открытых дверей. В идеале двери в кабинеты начальников должны быть открыты во всех организациях вне зависимости от их размеров.

ИНСТРУМЕНТ

ПОЛИТИКА ОТКРЫТЫХ ДВЕРЕЙ НА МИКРОПРЕДПРИЯТИИ

1. Руководителю целесообразнее выступить с конкретным и ясным заявлением о том, что работники могут спокойно и не переживая за свою безопасность говорить о своих подозрениях на неправомерное поведение.

2. О такой возможности работникам нужно регулярно напоминать.

3. Позаботьтесь и о том, чтобы информаторов и в самом деле не преследовали.

[15] Всемирная ассоциация следователей по делам о мошенничестве подробнее рассматривает распространение механизмов, в частности в отчете Nations on Occupational Fraud and Abuse за 2016 год.

В то же время по причине ограниченных ресурсов нагрузка на работника по регистрации и рассмотрению соответствующих случаев может оказаться слишком велика, особенно тогда, когда на предприятии нет конкретного механизма, а люди не стесняются, когда возникают подозрения, обращаться к руководителю, который и так занимается связанными с работой жалобами. Если сообщений будет накапливаться слишком много или расследования окажутся более объемными, чем предполагалось, пострадает основная работа или руководителя, или лица, которое занимается сообщениями, или их обоих.

В такой ситуации, а также в случае, если политики открытых дверей недостаточно, можно принять конкретные меры в поддержку информирования и профилактики неправомерного поведения.

ИНСТРУМЕНТ

ПРИНЦИПЫ МЕХАНИЗМА ИНФОРМИРОВАНИЯ НА МАЛОМ И СРЕДНЕМ ПРЕДПРИЯТИИ

Если культура компании не поддерживает открытого обсуждения подозрений и работники из страха преследований держат их, скорее, при себе, то при создании механизма информирования на VKE следует обратить внимание в первую очередь на следующее:

Разница между информированием о неправомерном поведении и жалобами, связанными с работой	Информирование предполагает своей причиной ущерб общественным интересам. Например, могут сообщать об игнорировании техники безопасности и о том, что коллективу что-то угрожает. Если жалоба связана с работой, то речи об общественных интересах не идет, а работника может, например, раздражать то, что его начальник якобы к нему придирается. Ресурсы малого предприятия ограничены, и нужно тщательно взвесить возможность одновременного адекватного рассмотрения и сообщений о неправомерном поведении, и жалоб в связи с работой. Если жалоб становится слишком много, на их рассмотрение можно назначить кого-нибудь дополнительно.
Работники и руководители понимают свои роли	Сделайте так, чтобы за механизм информирования отвечал конкретный человек. Обеспечьте для информирования наличие как минимум трех альтернативных каналов: 1. непосредственный начальник;

	2. коллега; 3. конфиденциальный канал (почтовый ящик, телефон, веб-форма и т.п.). Позаботьтесь о том, чтобы начальники на местах поддерживали информирование и понимали, что им нечего обижаться, если подчиненный сообщил о чем-то через их голову и предпочел, например, автоответчик или доверенное лицо. Подробнее в разделе Распределение ролей
Обеспечение конфиденциальности	Чем меньше коллектив, тем сложнее при информировании обеспечить конфиденциальность, поскольку у всех свои специфические рабочие обязанности. Можно предположить, что сообщение будет содержать информацию, позволяющую без труда установить его автора. Позаботьтесь о том, чтобы конфиденциальность распространялась не только на содержание сообщения, но и на сам факт его наличия. Это значит, что о поступившем сообщении должно знать как можно меньше людей.
Преимущества независимой горячей линии	При управлении механизмом информирования в экономии ресурсов может помочь аутсорсинг. Например, можно заказать услугу горячей линии или справочного телефона на стороне, и подрядчик должен будет обеспечивать конфиденциальность информатора и самого сообщения.
Информирование о нарушении	Сообщить о нарушении должно быть просто. Разъясните вкратце, кто может информировать (и рассчитывать на конфиденциальность), о чем и по каким каналам. Это разъяснение разместите так, чтобы работники обязательно его видели (например, на баннере в интранете, на сайте, на плакатах или флаерах в офисе, на производстве). Регулярно напоминайте работникам о возможностях и каналах информирования.

Крупные и международные компании отличаются обычно большими коллективами, связанными с трансграничной торговлей рисками и/или большим оборотом, в силу чего наличие развернутого и продуманного механизма информирования должно быть само собой разумеющимся, и состоять он должен из инструкции по информированию, при необходимости – из разных каналов информирования, а также регулярного повышения осведомленности через обучающие занятия и продуманную коммуникацию.

Если на предприятии разноязычный коллектив, вся информация и все каналы должны переводиться.

Риски неэффективной системы

Если работник целенаправленно занимается присвоением ресурсов предприятия, неправомерно или как-нибудь еще некорректно ими пользуется, нужно иметь в виду, что раскрыть его может оказаться непросто. Как и преступник, такой работник сознательно скрывает свою деятельность.

Но чаще всего неправомерное поведение не является умышленным, оно может иметь место **по незнанию.** Тем важнее продуманность существующих механизмов, чтобы работники могли эффективно сообщать о своих подозрениях.

Если на предприятии не создано ясных механизмов и у работников отсутствует возможность безопасного информирования, предприятию будет сложно управлять потенциальными рисками. Если работники этим механизмам не доверяют, они, вероятно, будут всё скрывать, и предприятие не узнает о рисках, угрожающих самой компании, ее акционерам или пайщикам либо общественности. Молчание не позволит предприятию заняться проблемой и предотвратить ущерб. Если механизм информирования вызывает сомнения, на предприятии могут узнать о проблеме уже от следственных органов, адвокатов или через СМИ, потому что работник, скорее всего, обратится именно к ним.

Упущенные по причине слабой системы возможности связаны и с расходами, которые могут быть значительными: штрафы, компенсации, высокие страховые выплаты, следственные действия компетентных органов, незаключенные договоры, неполученная прибыль, а в крайнем случае даже потерянные жизни.

Если произойдет серьезное несчастье, а то и катастрофа, и выяснится, что компания пыталась помешать информированию, игнорировала его и занималась в связи с этим запугиванием, – под угрозой окажется не только репутация предприятия, но и его дальнейшая деятельность.

Поскольку как можно раньше узнавать о неправомерном поведении – в интересах предприятия, механизм должен быть соответствующим образом настроен. Ясные процессы, сферы ответственности и помощь со стороны руководства помогут обеспечить, чтобы механизм был эффективным, работникам было просто им пользоваться, а информирование о неправомерном поведении поддерживалось.

ЯСНЫЕ ПРОЦЕССЫ

Кто может быть информатором?

При создании каналов информирования важно установить, кто может сообщать о своих подозрениях и при этом рассчитывать на защиту со стороны предприятия, например на обеспечение конфиденциальности. Защита информаторов может распространяться не только на работников предприятия, но и на других лиц, например на тех, кто работает по договору подряда, работников подрядчика, посредников, волонтеров, практикантов и членов совета. В интересах предприятия побуждать всех их сообщать о неправомерном поведении.

Защита может распространяться и на общественность, например на клиентов.[16] То, насколько масштабной может быть защита, в эстонских условиях зависит в первую очередь от имеющихся в распоряжении предприятия ресурсов, поскольку законодательные обязательства по защите информаторов на частные компании не распространяются.

Не стоит недооценивать и тот факт, что широкая общественность и клиенты располагают информацией о неправомерном поведении на предприятии и, таким образом, являются важными сторонами в деле предотвращения такого поведения. Поэтому имеет смысл позволить и им быть информаторами.

РЕКОМЕНДАЦИЯ

НАЗНАЧЕНИЕ ИНФОРМАТОРОВ

1. Установите, кто на предприятии может конфиденциально пользоваться каналами информирования.

2. Подумайте, достаточно ли у предприятия ресурсов, т. е. людей, времени и денег, чтобы поддерживать всех информаторов.

О чем сообщать?

Компания должна ясно описать, о каком неправомерном поведении можно сообщать через каналы информирования. Обычно пытаются разделить неправомерное поведение, которое влияет на клиентов, население или работодателя, и т. н. жалобы в связи с рабочим местом.

Недостойное деяние	Жалоба по работе
Касается других	Касается жалующегося
Вредит общественным интересам	Вредит жалующемуся

[16] Проведенное в 2010 году PriceWaterhouseCoopers исследование показало, что 55% опрошенных предприятий распространяло защиту информаторов и на сторонних лиц, таких как подрядчики, поставщики и т.п., а 35% – и на широкую общественность.

Недостойное деяние	Жалоба по работе
Достаточно сообщения и свидетельства, доказывать не требуется	Необходимо доказать

В обоих случаях можно задействовать отдельные каналы и лиц, занимающихся расследованием, если

1. расследование, возможно, придется вести по разным процедурам, или
2. на лицо, ведущее расследование падает слишком большая нагрузка.

ПРИМЕР

СИСТЕМА TALLINNA VESI AS[17]

В этом документе приведены примеры неправомерного поведения, о котором следует сообщать.

Неправомерное поведение, о котором работник знает или подозревает, которое могло иметь место или имеет место и на которое распространяется настоящий Порядок, – это:

1. Финансовое или бухгалтерское мошенничество, коррупция, взяточничество или иное ненадлежащее деяние или поведение в финансовой сфере.
2. Недостаточный внутренний контроль на Предприятии или имеющие на нем место крупные аудиторские или бухгалтерские недочеты, которые могут иметь важное или заметное влияние на финансовые результаты Предприятия.
3. Конфликт интересов или неэтичное поведение либо недостаток профессионализма или осмотрительности, например покупка чего-либо у принадлежащего родственнику предприятия или сотрудничество с предприятием, акционером которого лицо является, а также фальсификация данных в коммерческих целях.
4. Использование инсайдерской информации при торговле акциями AS Tallinna Vesi или другого предприятия.
5. Ненадлежащее использование конфиденциальной или деликатной коммерческой информации.
6. Непредоставление внутри Предприятия, или регуляторам Предприятия, или другим соответствующим органам подлежащих предоставлению сведений или уничтожение соответствующих документов.
7. Любого рода преступление или неисполнение юридических обязательств от лица Предприятия.
8. Нарушение условий выданных Предприятием разрешений и лицензий.
9. Создание угрозы или причинение ущерба чьему-либо здоровью и безопасности на работе.
10. Неинформирование о ситуации, в которой ясно, что наша деятельность причинила или может причинить ущерб либо в виде загрязнения, либо иным образом.
11. Несоблюдение порядков, процедур и внутренних правил Предприятия или Кодекса деловой этики.

[17] Порядок информирования о неправомерном поведении в AS Tallinna Vesi размещен на сайте предприятия: https://www.tallinnavesi.ee/wp-content/uploads/2017/05/2017-30-06-Whistleblowing-policyASTV-EST_uus-veeb.pdf.

12. Умышленное сокрытие любой относящейся к вышеприведенным темам информации.
13. Прочие серьезные подозрения.

Работникам стоит разъяснить, что **бездействие тоже** может рассматриваться как ненадлежащее деяние. Например, руководитель строительного проекта оставляет без внимания жалобы в связи с безопасностью труда, ставя под угрозу весь коллектив.

Каждая организация сама решает, информации о каких проблемах она ждет, и вполне обычно, когда обо всех подозрениях сообщается по одному каналу.

ПРИМЕР

AS CIRCLE K ЖДЕТ ЛЮБЫХ СООБЩЕНИЙ

В международной сети комплексного обслуживания AS Circle K нет строгих ограничений, о чем работник может сообщать. По горячей линии или через доверенное лицо могут затрагиваться любые этические и т. н. серые темы. На предприятии действует правило, что за ошибочную информацию работнику ничего не будет, но гораздо хуже, если он о чем-то не сообщил и проступок остался нераскрытым.

В случае если предприятие решит, что всякого рода проблемами занимается один и тот же специалист, то важно, чтобы такое доверенное лицо понимало, когда речь идет о проступке, а когда – о жалобе по работе, чтобы человек мог задать правильные вопросы[18] и ничего не упустил.

[18] См. раздел Прием сообщений

Трилемма информатора

Важно помнить, что информатор – это обычный работник, на которого неожиданно свалился большой моральный груз. Если упрощенно, то перед ним три пути, каждый из которых вызывает много вопросов и требует принятия ряда решений.

Предприятие должно прилагать усилия ради того, чтобы работник со своими подозрениями обращался к коллеге или доверенному лицу, потому что только в таком случае предприятие сможет само заняться расследованием или решением потенциальной проблемы и наиболее эффективно снизить материальные и репутационные риски. Если работник ничего не делает или обращается, например, к СМИ, значит предприятие такую возможность упустило.

Ни один работник не хочет быть информатором, а если он до этого дошел, значит он об этом много размышлял. Ниже приведена упрощенная схема типичных причин, по которым не происходит информирования внутри предприятия, а работник, скорее, обратится куда-то еще.

РЕКОМЕНДАЦИЯ

ПОДДЕРЖКА ИНФОРМАТОРА

1. Помните, что в выявлении нарушений работник играет ключевую роль.

2. Подумайте, какие проблемы могут возникнуть на вашем предприятии у работника-информатора.

3. Найдите им решения и добавьте эти решения в свою инструкцию по информированию или регулярно разъясняйте их коллективу.

4. Не смешивайте информатора и информацию, мотивы информатора имеют второстепенное значение, приоритетом должно быть расследование содержания сообщения.

Как информировать?

Предприятие четко описывает, как подается жалоба:

1. устно или письменно;
2. по горячей линии, через почтовый ящик или веб-форму;
3. публично, конфиденциально или анонимно.

Проще всего разъяснить это в инструкции или каком-либо еще документе.

ИНСТРУМЕНТ

БАЗОВЫЕ ПРИНЦИПЫ ИНСТРУКЦИИ ПО ИНФОРМИРОВАНИЮ

Хорошая инструкция по информированию очерчивает однозначно понимаемые границы информирования о неправомерном поведении и его расследования, говорит о защите ценностей организации. В инструкции могли бы быть раскрыты следующие аспекты:

1. Компания относится к неправомерному поведению серьезно, и такому поведению имеется четкое определение.

2. Работник может информировать о неправомерном поведении, игнорируя субординацию.

3. Работник может конфиденциально посоветоваться с третьей независимой стороной.

4. При необходимости предприятие обеспечивает информатору конфиденциальность.

5. Процесс информирования вне предприятия.

6. Преследование информатора и клевета на него неприемлемы.

Принимая во внимание факторы, связанные со сферой деятельности, структурой и размером компании, в каждом отдельном случае следует самостоятельно решить, кто может использовать канал информирования и о каких проблемах сообщать.

Хорошая инструкция уже с самого начала поощряет информирование и успокаивает информатора (см., например, Трилемму информатора). Комплексная, простая в понимании и широко распространяемая инструкция является основой профилактики неправомерного поведения.

ИНСТРУМЕНТ

АЛЬТЕРНАТИВЫ ИНСТРУКЦИИ

Ответы на связанные с информированием вопросы можно найти, например, в кодексе этики предприятия или каком-либо другом аналогичном документе. Важно, чтобы информатор мог быстро найти необходимые указания.

ПРИМЕР

ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ В TELIA

Международное телекоммуникационное предприятие Telia Company разъясняет связанные с информированием, безопасностью и конфиденциальностью общие вопросы и приводит различные примеры и наработки в ЧЗВ[19], т. е. в документе о часто задаваемых вопросах, который просто найти на специальной, отделенной от серверов Telia Company странице[20] EthicsPoint[21].

Открытое, конфиденциальное и анонимное информирование

О неправомерном поведении можно сообщить тремя путями: публично, конфиденциально или анонимно.

ИНФОРМИРОВАНИЕ О НЕПРАВОМЕРНОМ ПОВЕДЕНИИ

	Публичное	**Конфиденциальное**	**Анонимное**
Личность информатора	Личность информатора известна всем	Личность информатора известна доверенному лицу, с разрешения информатора – и другим имеющим отношение к вопросу лицам	Личности информатора не знает никто
Влияние на расследование	Информатору можно задавать уточняющие вопросы	Информатору можно задавать уточняющие вопросы	Задать уточняющие вопросы невозможно
Обеспечение защиты информатора	Информатора можно защитить от преследований, личность информатора публична	Личность информатора можно держать в тайне, информатора можно защитить от преследований	Личность информатора неизвестна, поэтому принятие мер защиты затруднительно

[19] https://secure.ethicspoint.eu/domain/media/et/gui/101615/faq.pdf

[20] https://secure.ethicspoint.eu/domain/media/ru/gui/101615/index.html

[21] EthicsPoint – торговая марка международной компании NAVEX, предлагающей решения линий доверительной связи, о чем подробнее можно узнать здесь: https://secure.ethicspoint.com/domain/ru/default_reporter.asp

В случае публичного информирования работник не просит о конфиденциальности, и имеющие отношение к делу лица знают суть вопроса и кто его поднял. Открытость помогает лучше оценить ситуацию и решить, что делать дальше.

В идеале работники смело и открыто говорят о своих опасениях и подозрениях. Они знают, что руководство относится к их жалобам серьезно и заботится о том, чтобы после сделанного сообщения не было преследований со стороны коллег или начальства. Такие организации встречаются очень редко, поскольку размер предприятия, связанные со сферой его деятельности риски, репутация информатора в обществе и в самой организации оказывают влияние на то, насколько люди склонны в открытую говорить о проблемах.

В случае конфиденциального сообщения работник раскрывает свое имя, однако хочет, чтобы в ходе расследования оно без его согласия не всплывало. Конфиденциальное сообщение позволяет обращаться к информатору для уточнения обстоятельств или за комментариями. Эксперты[22] единодушны во мнении, что если о неправомерном поведении открыто говорить невозможно, то конфиденциальное сообщение – это лучшая альтернатива.

Компания должна делать всё от нее зависящее, чтобы обеспечить обещанную конфиденциальность. В противном случае работники утратят доверие к каналу информирования, перестанут им пользоваться, и факты неправомерного поведения останутся невскрытыми.

При анонимном информировании личность информатора неизвестна, что затрудняет выяснение обстоятельств неправомерного поведения, а также обеспечение защиты информатора. С лицом, передавшим анонимное сообщение, связаться для уточнения обстоятельств и для комментариев, как правило, невозможно.

Исключением являются веб-платформы и автоответчики, которые выдают информатору уникальный PIN-код, по которому информатор потом может проверить, отреагировали ли на его сообщение. В таком случае у информатора может иметься возможность ответить на возникшие вопросы.

ПРИМЕР

ОБРАТНАЯ СВЯЗЬ С (АНОНИМНЫМ) ИНФОРМАТОРОМ

Ramirent – предлагающая аренду оборудования международная компания принимает сообщения через интернет-платформу[23], в которой информатор может оставаться полностью анонимным, однако позже с ним возможно связаться. Это возможно благодаря специальному коду доступа.

Информатор отправляет через платформу сообщение и получает уникальный код. Этот код позволяет потом сделать в системе запрос, чтобы посмотреть, есть ли по делу какие-нибудь подвижки.

В большинстве случаев анонимное информирование не поощряется, и в соответствующей инструкции указывается, что в таком случае может оказаться невозможным как-то защитить

[22] Public Concern at Work, статья 10; TI 2013 International Principles for Whistleblower Legislation, пункт 7.

[23] Подробнее о системе Ramirent: https://wrs.expolink.co.uk/client-EjoZdWMo

информатора, однако, если после сообщения личность его станет известна, предприятие все равно должно принять меры по его защите[24].

В случае если компания все-таки готова принимать и анонимные сообщения, в инструкции следует разъяснить, что такие сообщения должны быть максимально подробными.

РЕКОМЕНДАЦИЯ

СПОСОБ ИНФОРМИРОВАНИЯ И ЗАЩИТА

Обеспечьте, чтобы работники знали, в случае какого способа информирования им будет гарантирована конфиденциальность.

Каналы информирования

Каналы информирования бывают разные, и каждая организация сама должна решить, достаточно ли ей одного или нужно несколько.

Имеет смысл, например, открыть **горячую линию, электронный адрес** или **веб-платформу** для приема конфиденциальных сообщений.

Некоторые предприятия используют **физические почтовые ящики,** в которые работники могут опускать анонимные или конфиденциальные сообщения. Систем с использованием бумажных носителей постепенно становится всё меньше, поскольку современные интернет-решения также обеспечивают анонимность.

ПРИМЕР

ПОЧТОВЫЕ ЯЩИКИ «ANNA TEADA» В EESTI ENERGIA

На офисных зданиях AS Eesti Energia и Elektrilevi, а также на производственных объектах в Ида-Вирумаа есть стенды и почтовые ящики «Anna teada» («Сообщи»), через которые работники могут в числе прочего информировать о неправомерном поведении.

Каналы информирования должны быть доступны всем, от кого предприятие ждет сообщений. Это значит, что **предприятие использует такие каналы, которые привычны для целевых групп.** Например, если часть персонала вообще не работает с компьютерами, то только лишь веб-платформы или электронного адреса будет мало, работников это ни к чему не побудит.

[24] TI 2013 International Principles for Whistleblower Legislation, пункт 13.

ПРИМЕР

ОТКРЫТАЯ ГОРЯЧАЯ ЛИНИЯ НА PEPSICO

Ответственное предприятие, независимо от своего размера, обращает внимание и на свои цепочки поставок и связанные с ними риски.

Для снижения рисков имеет смысл позволить работникам входящих в цепочку поставок предприятий тоже сообщать о проблемах, либо создав открытую для всех горячую линию, либо потребовав от поставщиков наличия механизма информирования.

Например, концерн PepsiCo, одно из ведущих европейских предприятий по выпуску продуктов питания и напитков, создал «этический» канал, открытый для всех, кто подозревает что-то противозаконное или противоречащее ценностям компании.[25]

Важно, чтобы:

1. канал информирования администрировался независимо (например, доверенным лицом работников или сторонним провайдером), а жалобы передавались руководству на условиях конфиденциальности;
2. была обеспечена возможность анонимного информирования;
3. ставшие известными случаи рассматривались конфиденциально, чтобы обеспечить соответствующую защиту как информатору, так и лицу, в отношении которого была подана жалоба;
4. каждая жалоба рассматривалась тщательно, и участвующие в рассмотрении лица ставились бы в известность о ходе дела;
5. в отношении регистрации, документирования и рассмотрения жалоб была установлена четкая процедура.[26]

У большинства крупных международных организаций механизм информирования есть, однако значительная часть предприятий не в состоянии обеспечить защиту своих работников от преследований.[27]

Поэтому для крупных организаций, действующих на международной арене, вопрос не в том, должен ли у них быть механизм информирования, а, скорее, в том, **как побудить людей к информированию, как эти сообщения эффективно обрабатывать и как защитить информаторов от преследований.**

[25] Кодекс поведения PepsiCo размещен здесь: https://pepsico.ee/assets/pdf/Estonian-Global-Code-of-Conduct.pdf, о неправомерном поведении можно сообщить здесь: https://secure.ethicspoint.com/domain/media/en/gui/52943/index.html

[26] MTÜ Korruptsioonivaba Eesti. Руководство по предотвращению коррупции для частного сектора.

[27] Business Case for Speaking Up, стр. 2.

ИНСТРУМЕНТ

СОЗДАНИЕ КАНАЛОВ ИНФОРМИРОВАНИЯ НА МЕЖДУНАРОДНОМ ПРЕДПРИЯТИИ

Вне зависимости от размеров предприятия создание любого канала информирования может показаться сначала ресурсоемким и сложным. Корпорация, ведущая международный бизнес, должна учитывать коррупционные риски в разных странах, языковой вопрос и инфраструктуру.

В странах с высоким риском коррупции определяющую роль играет местный контекст, поэтому важно обеспечить, чтобы

1. каналы информирования были доступны всем работникам и поставщикам,

2. а сообщения рассматривались строго конфиденциально и эффективно.

Компания, действующая в разных странах, может предложить своим работникам широкий выбор каналов информирования – например, возможность обратиться непосредственно к доверенному лицу, к консультанту или в комиссию по этике, через веб-платформу, по телефону горячей линии или по электронной почте.

Каналы информирования должны быть бесплатными, доступными всегда и на всех рабочих языках предприятия.

Если компания хочет, чтобы информаторы могли адресовать свои сообщения за пределы предприятия, стоит найти специалистов, которые

1. предлагают услуги администрирования таких сообщений,

2. работают на международном уровне и/или

3. имеют очень хорошее представление о местной ситуации.

В качестве альтернативы можно обратиться к местным волонтерским объединениям, одной из основных сфер деятельности которых является поддержка каналов информирования, консультирование информаторов и администрирование жалоб. Например, хорошими исходными возможностями располагают местные дочерние организации Transparency International.

Если предприятие работает в нескольких странах, то особенно рентабельным считается аутсорсинг услуги горячей линии. Чаще всего провайдер заботится и о том, чтобы предприятие получало расшифровку (транскрибацию) сообщений на языке оригинала и их перевод, например на английский.

ПРИМЕР

ВЕБ-ПЛАТФОРМЫ

БЕСПЛАТНЫЕ

GlobaLeaks[28] – бесплатное программное обеспечение, позволяющее организациям предлагать своим работникам безопасный канал информирования.

Решение GlobaLeaks бесплатное, поэтому это первый кандидат для внедрения веб-платформы.

ПЛАТНЫЕ

Работающие в Эстонии компании чаще всего используют следующие решения:

1. Expolink[29]
2. Navex[30]
3. WhistleB[31]

ОТЕЧЕСТВЕННЫЕ

Услуги администрирования горячих линий предлагают крупнейшие эстонские консалтинговые и адвокатские бюро.

Прием сообщений

Предприятие заботится о том, чтобы работники знали, кто принимает их сообщения, в т. ч. **кто еще их получает,** кроме непосредственного начальника (доверенное лицо, внутренний контроль и т.п.). Эти лица должны уметь правильно принять сообщение, зарегистрировать его и обеспечить информатору конфиденциальность.

В задачу лица, принимающего сообщения, входит управление ожиданиями информатора. При получении сообщения человек, который его принял, должен подумать о том, чего хотел достичь информатор. Иногда информатор хотел просто, чтобы кто-то разобрался в сомнительной ситуации, а иногда – чтобы о проблеме заговорили открыто. Нередки и случаи, когда информатор надеется, что работник, который повел себя некорректно, будет уволен. Человек, который принял сообщение, должен объяснить информатору, как предприятие разбирается с подозрениями и какими могут быть реальные результаты.[32]

При получении сообщения о неправомерном поведении принимающее лицо должно:

1. уведомить информатора о получении сообщения;
2. воздержаться от предвзятости и учесть свой уровень знаний о том, что касается неправомерного поведения;
3. рассмотреть поступившее сообщение надлежащим образом;
4. соблюдать требование конфиденциальности;

[28] https://www.globaleaks.org/

[29] https://www.expolink.co.uk/our-clients/case-studies/yorkshire-building-society/

[30] https://www.navexglobal.com/en-us/products/hotline-reporting-and-intake

[31] https://whistleb.com/whistleblowing-software/

[32] Разъяснительная работа поможет составить т. н. путь сообщения: ПРИЛОЖЕНИЕ 2. ПРИМЕР ДВИЖЕНИЯ СООБЩЕНИЯ

5. при необходимости принять меры по защите информатора;
6. обеспечить справедливое обращение с подозреваемым лицом;
7. сообщить информатору о результатах расследования.

ИНСТРУМЕНТ

ИНСТРУКЦИЯ ПО ПРИЕМУ СООБЩЕНИЯ

Принимая устное сообщение:

a) постарайтесь найти для беседы приватное помещение;

b) делайте заметки только с согласия информатора;

c) задавайте открытые вопросы (кто, что, где, когда и почему). Постарайтесь установить как можно больше фактов. В числе наводящих вопросов можно использовать следующие:

- почему информатор решил сообщить о неправомерном поведении?
- кому уже сообщено о неправомерном поведении?
- что информатор имел в виду под неправомерным поведением?
- где и когда имело место неправомерное поведение?
- кто связан с инцидентом?

d) когда информатор ожидает обратной связи? Если человек не получит никакой обратной связи, он может подумать, что вопросом и не занимались, и решит обратиться куда-то еще, например к журналистам. Информатора нужно по возможности держать в курсе расследования, поскольку это поможет оправдать его ожидания, предотвратить проблемы и даст ему понять, что всё идет хорошо;

e) поясните, что с вопросами или за дополнительной информацией информатор может обратиться к лицу, принявшему сообщение.

РЕКОМЕНДАЦИЯ

ПРИЕМ СООБЩЕНИЙ ПО ЭЛЕКТРОННОЙ ПОЧТЕ, ПО ГОРЯЧЕЙ ЛИНИИ ИЛИ ЧЕРЕЗ ВЕБ-ПЛАТФОРМУ

Позаботьтесь о том, чтобы для сообщений по электронной почте, по горячей линии или через веб-платформу имелась продуманная подробная анкета, отвечая на вопросы которой, информатор предоставит все необходимые для расследования сведения.

Помните, что информатор может больше и не выйти на связь и что-нибудь уточнить может оказаться невозможным. Поэтому важно с самого начала получить как можно больше данных.

ПРИМЕР

ВЕБ-АНКЕТА RIIGI KINNISVARA AS

RKAS использует простую форму интернет-анкеты, в которой информатора просят указать время и место инцидента, сам инцидент и объяснить происхождение информации. При желании можно оставить и свои контактные данные.[33]

Время инцидента Пожалуйста, укажите дату (дд/мм/гггг) и время. Если точное время неизвестно, укажите примерно или с точностью до месяца или года.

Место инцидента Пожалуйста, как можно точнее опишите, где произошел инцидент (страна, уезд, город/волость, район, адрес). По возможности уточните название связанного с инцидентом структурного подразделения.

Описание инцидента Пожалуйста, как можно точнее опишите обстоятельства инцидента, в т. ч. какова была Ваша роль, кто еще имеет отношение к инциденту (имена, фамилии и должности), какова Ваша оценка причиненного ущерба и его ориентировочная сумма (в евро), в чем источник опасности и кто его создал. (Если желаете представить доказательства, пожалуйста, отправляйте их на анонимный адрес rkas@ee.ey.com).

Происхождение информации Пожалуйста, опишите источник информации. В случае если Вы сами не были свидетелем инцидента и информация о нем стала Вам известна через других лиц, укажите, пожалуйста, их имена, фамилии и контактные данные. Если факт инцидента подтверждается документами, фотографиями или видео, представьте их перечень и краткое описание.

Контактные данные При передаче сообщения Вы можете сохранить анонимность. Если Вы хотите сделать сообщение от своего лица, пожалуйста, укажите свои основные контактные данные (имя, фамилию, номер телефона и/или адрес электронной почты). Ваши контактные данные нужны только изучающей сообщение независимой стороне. Контактные данные требуются для того, чтобы в ходе расследования запросить дополнительную информацию. Ни на каком этапе процесса Ваша личность не будет раскрыта без Вашего согласия.

Иногда для подкрепления сообщения информаторы хотят предъявить различные документы. Позаботьтесь о том, чтобы передача файлов не угрожала конфиденциальности информатора, например, не стоит просить его пересылать файлы по электронной почте, потому что тогда установить отправителя бывает просто.

[33] Анкета информатора Riigikinnisvara AS доступна здесь: https://emeia2.ey-vx.com/survey/TakeSurvey.asp?PageNumber=1&SurveyID=3KIn531Hlp2K285.

ПРИМЕР

БЕЗОПАСНАЯ ПЕРЕДАЧА ДОКАЗАТЕЛЬНЫХ МАТЕРИАЛОВ

Прикреплять файлы позволяет, например, бесплатная платформа GlobaLeaks. Через нее информатор может передать дополнительные данные, и факт сообщения останется конфиденциальным.

Лица, принимающие сообщения, должны учитывать свои знания в том, что касается неправомерного поведения, и то, какими сведениями информатор готов поделиться.

РЕКОМЕНДАЦИЯ

ЧТО НУЖНО ЕЩЕ УЧИТЫВАТЬ, ПРИНИМАЯ СООБЩЕНИЯ?

Лицо, принимающее сообщение, должно оценить:

- серьезность и срочность случая;
- следует ли заниматься инцидентом по инструкции об информировании о неправомерном поведении или по какой-либо другой инструкции;
- требуется ли помощь других менеджеров или специалистов;
- если инцидент носит деликатный характер, число привлекаемых к его рассмотрению лиц должно быть как можно меньше;
- если в отделе информатора требуется провести опрос, информатора следует предупредить, чтобы он был готов отвечать наравне с другими;
- если информатор опасается преследований, ему следует при первой возможности снова обратиться к доверенному лицу или к непосредственному начальнику, которые должны быть готовы его успокоить или связаться с отделом по работе с персоналом, чтобы разрешить ситуацию.

После получения сообщения нужно принять решение о дальнейших действиях. Передайте информатору, что:

1. речь не идет о неправомерном поведении и организация не будет заниматься расследованием инцидента (обоснуйте)

ИЛИ

2. сделайте одно из следующего:
    1. примите дисциплинарные меры без расследования, сообщив об этом информатору и обосновав такое решение;
    2. срочно примите превентивные меры (например, временно отстраните работника от работы), начните расследование, сообщив об этом информатору и обосновав такое решение;
    3. приступите к расследованию и/или
    4. сообщите следственным органам.

Защита информатора

Во многих исследованиях предприятиям рекомендуется способствовать т. н. открытому информированию, потому что так проще работать с поступающими сообщениями и снижается опасность возникновения в коллективе атмосферы недоверия. Возможно и анонимное информирование, но в таком случае сложно обеспечить защиту информатора и задавать дополнительные вопросы.[34] Тем не менее, у информатора должно сохраняться **право на конфиденциальность,** которое лучше всего помогает в защите от возможных преследований и других угроз, при этом предприятие сохраняет возможность деликатного рассмотрения жалобы.

В инструкции по информированию о неправомерном поведении может подчеркиваться **недопустимость преследований** за сообщение и помощь в расследовании. Предприятия, которые уже привлекли значительные ресурсы для побуждения работников к тому, чтобы сообщать о неправомерном поведении, должны стратегически заниматься и профилактикой возможных преследований, а также решением вопроса о поддержании среди работников доверия к механизму информирования.

РЕКОМЕНДАЦИЯ

После получения сообщения, продолжайте общаться с работником, как раньше:

- поддерживайте нормальное рабочее общение;
- оценивайте работника по его результатам;
- давайте работнику такие же, что и раньше, задания;
- предоставляйте необходимую для повседневной работы информацию;
- приглашайте работника на коллективные мероприятия, например на традиционные совместные обеды, рождественские праздники, дни рождения и т. п.

Работника нужно предупредить, что, если он хочет сохранить конфиденциальность, ему нельзя обсуждать факт и содержание сообщения с коллегами, потому что в таком случае никакой конфиденциальности не будет.

Если информатор подозревает, что его могут начать преследовать, то обязанностью лица, получившего сообщение, является заверить, что к нему можно обращаться и по поводу преследований. Иногда, чтобы успокоить человека, требуется отдельная беседа.

Управление ситуацией

Действенное и адекватное управление ситуацией является важной частью механизма информирования. Рассмотрение подозрений на неправомерное поведение может поначалу отпугивать, но, если следовать рекомендациям, основанным на передовом опыте, с сообщениями можно работать квалифицированно и эффективно.

Эффективное управление ситуацией характеризуется:

- наличием независимых и проактивных лиц, которые принимают сообщения, корректно отвечают информатору и дают указания другим сторонам;

[34] И при анонимном информировании следует обеспечивать конфиденциальность сообщения, потому что по его содержанию можно вычислить личность информатора. Это особенно важно для малых и средних организаций.

- обеспечением конфиденциальности;
- понятным «путем» сообщения;
- ясными критериями, определяющими время и способ общения с информатором и другими сторонами;
- региональной и функциональной координацией, а также
- сбором данных с целью помочь организации в разрешении ситуаций, выявлением закономерностей возникновения проблем и подотчетности совету и акционерам.

РЕКОМЕНДАЦИЯ

Если выяснится, что неправомерное поведение является, по всей видимости, противозаконным, поставьте в известность полицию и прекратите расследование внутри организации, потому что оно может помешать работе следственных органов.

Ответственное за механизм лицо устанавливает и критерии в отношении того, когда и на каких основаниях прекращается расследование инцидента.

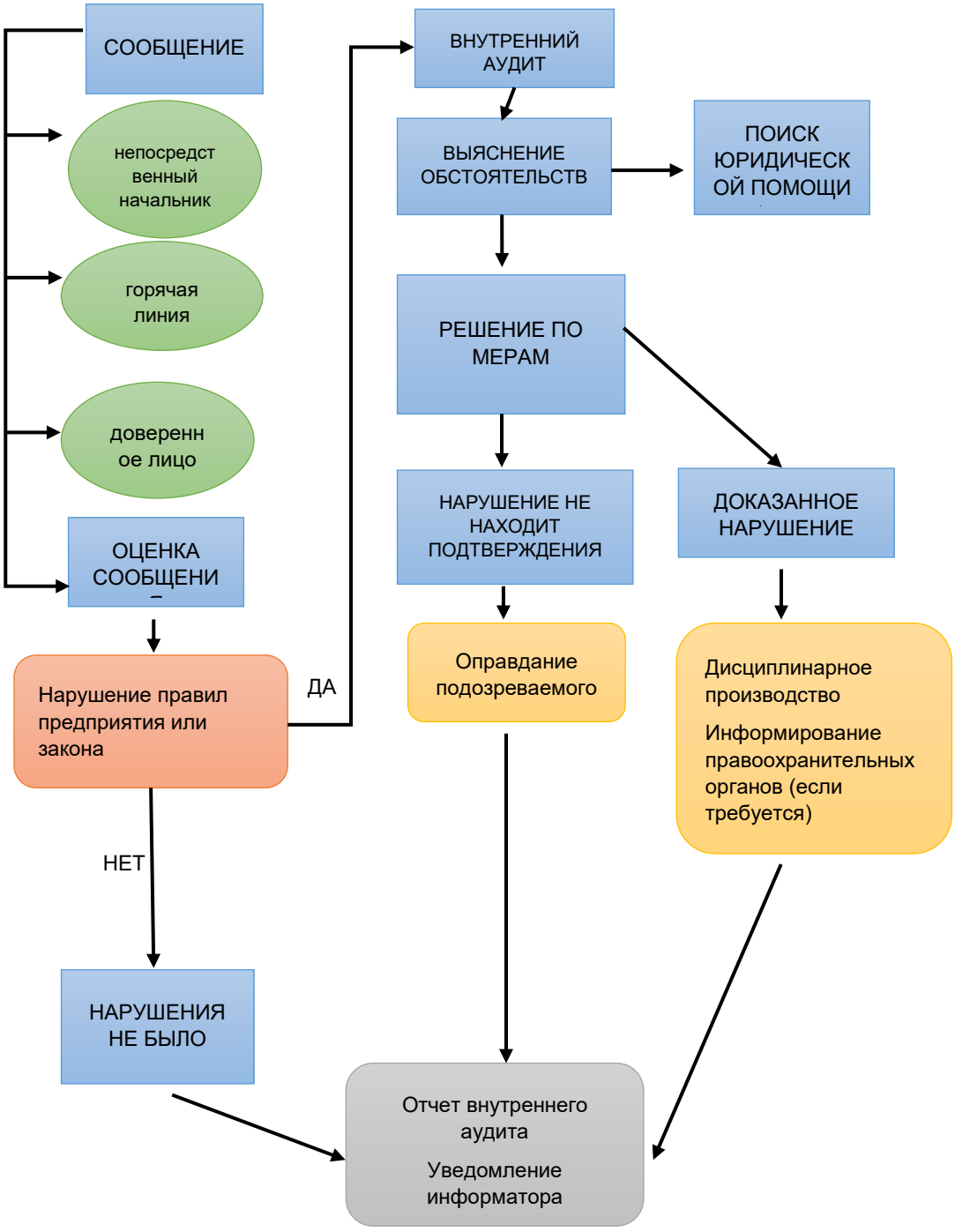
РЕКОМЕНДАЦИЯ

КОМИССИЯ ПО ЭТИКЕ

Мероприятия по расследованию не всегда позволяют прийти к конкретным выводам, а решение о прекращении рассмотрения инцидента может принимать комиссия по этике в составе, например, собственника, исполнительного директора и представителя юридического отдела.

Путь сообщения в крупной организации

Рассмотрение сообщений в крупных и малых организациях осуществляется сходным образом. В крупных организациях, возможно, существует, например, внутренний аудит или юридический отдел с правом на расследование. На приведенной схеме показан путь сообщения в таких компаниях. В малых организациях ответственность за рассмотрение сообщений лежит на лице, которое отвечает за соответствующий механизм.



Злоупотребление механизмом

В отношении любого механизма существует риск его использования в корыстных целях. Механизм информирования и связанная с ним защита информатора не являются исключением. В то же время исследования показали, что тривиальные или лживые

сообщения встречаются довольно редко.[35] Инструкция по информированию может заранее предусматривать санкции в отношении работников, которые сознательно используют механизм для создания ложных подозрений. Эти принципы должны применяться последовательно.

РЕКОМЕНДАЦИЯ

1. Добавьте в инструкцию по информированию или в какой-либо другой соответствующий документ заявление, что компания не приемлет выдвижения заведомо ложных подозрений.

2. Не нарушайте это обещание!

[35] Transparency International (2007) The Business Case for «Speaking Up». How Internal Reporting Mechanisms Strengthen Private-Sector Organisations.

ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

Механизм информирования может выглядеть образцовым и хорошо продуманным, но от него не будет пользы, если работники о нем не знают.

Предприятия стараются повышать осведомленность работников. Это можно делать разными способами, например с помощью плакатов в местах общего пользования или объявлений в интранете, напоминающих о том, что о своих подозрениях следует сообщать.

ПРИМЕР

АКЦИЯ TELIA COMPANY «НЕ ДЕЛАЙТЕ ЭТОГО НА РАБОТЕ»

В Telia Company придумали юмористический «сериал» «Не делайте этого на работе»[36] (Don't do this at work), состоящий из 17 анимаций, на которых с огоньком показано то, чего на работе следовало бы избегать. Например, не следовало бы принимать на работу членов семьи, брать дорогие подарки, давать взятки и т. п.

Анимации выложены в формате GIF, их легко использовать в качестве баннеров в интранете, как заставки и в соцсетях.

Если у предприятия есть инструкция по информированию или документ, в котором описывается такая политика, они должны быть доступны работникам во внутренней сети, в руководствах, в пакетах, выдаваемых новичкам, и т. д. Информацию должно быть просто найти, работник, который раздумывает, сообщать или не сообщать, не должен сильно напрягаться в поисках того, к кому и куда обратиться.

РЕКОМЕНДАЦИЯ

Наряду с подробной инструкцией по информированию о неправомерном поведении или правилами составьте еще и такую инструкцию, которая помещалась бы на одну страницу и содержала бы следующее:

1. Призыв
2. О чем можно сообщать?
   - Перечислите примеры неправомерного поведения
3. Как можно сообщать?
   - Номер телефона, адрес электронной почты, веб-формы и т. п.

Краткие указания, возможно, в виде плаката, воспринимаются гораздо легче.

При коммуникации лучше ссылаться на сокращенный вариант инструкции.

Работники **будут доверять** механизму информирования, если:

1. действует политика открытых дверей;

[36] «На делайте этого на работе»: http://dontdothisatwork.teliacompany.com/

2. сообщения рассматриваются эффективно;
3. предприятие придерживается своей политики по данному вопросу и
4. руководство подает пример.

Добросовестные сообщения должны рассматриваться корректно, сложные случаи не должны игнорироваться или скрываться. Наоборот: сложные и деликатные случаи позволят убедиться, что установленные принципы работают и служат достижению целей компании.

Открытость – это самая безопасная для предприятия стратегия, и хороший механизм информирования подчеркивает и поддерживает приверженность ей. Если предприятие не соблюдает принципов и шлет неясные сигналы, например предоставляет работникам, надзорным органам или акционерам вводящие в заблуждение сведения о каком-либо случае неправомерного поведения, оно демотивирует людей и подрывает к себе доверие, а без этого механизм информирования работать не может.

СЛЕДУЕТ УЧЕСТЬ

Доверие к механизму информирования снижается, если предприятие позволяет им злоупотреблять или пытается заставить замолчать какого-либо информатора. Скорее всего, коллектив узнает об этом, что повлияет на мнения людей и их доверие к организации в целом и механизму информирования в частности.

Регулярная коммуникация

Практика показывает, что для поддержания функционирования механизма работникам нужно не реже раза в год напоминать, что такой механизм вообще существует, и объяснять, как он работает. Это можно делать каким-либо одним или несколькими из следующих способов:

1. Вкратце знакомить на собраниях или в рассылках с касающимися информирования темами, которые в позитивном ключе нашли отражение в СМИ.

2. Проводить среди работников опросы, чтобы оценить доверие к механизму информирования, знания о нем и связанный с ним опыт.

3. Разместить в интранете ответы на часто задаваемые вопросы по информированию (ЧЗВ).

4. Подчеркивая ценности и этические принципы предприятия, разъяснять и роль информирования.

5. Создавать и дополнять инструкции для работников всех уровней.

6. Сделать так, чтобы руководители и другие лица, которые принимают сообщения, могли где-нибудь консультироваться.

7. Предложите коллективу обзор того, как механизм до сих пор работал.

8. Предложите коллективу обзор того, какие уроки предприятие из этих ситуаций извлекло.

ПРИМЕР

ИНТЕРВЬЮ В ИЗДАНИЯХ ПРЕДПРИЯТИЯ И НА ВНУТРЕННЕМ РАДИО

AS Eesti Energia использует для распространения своих сообщений, в частности, интранет, внутреннее радио и собственную газету, и в интервью, которые там публикуются или передаются, заходит речь и о важности информирования, когда работников призывают сообщать о неправомерном поведении.

Материалы для повышения сознательности и осведомленности следует пересматривать, дополнять или менять раз в год или чаще, особенно если выясняется, что сознательность и осведомленность падают или контактные данные больше не работают.

Проблема	Решение	Инструмент
Работники не в курсе темы информирования	Привлеките работников к разработке механизма информирования	Опрос для определения осведомленности
	Обращение руководства к работникам	Побуждающая к информированию разъяснительная речь на собрании или семинаре
		Сделайте в рассылке обзор материалов СМИ, имеющих отношение к данной теме
	Убеждение новых работников[37]	Приложите инструкцию или ЧЗВ по информированию к материалам для нового работника
		Добавьте тему во вводный инструктаж нового работника

[37] Проведенное в 2018 году исследование Protect UK показало, что 39% информаторов – это новые работники, которые, в отличие от старожилов, свежим глазом лучше замечают неправомерное поведение.

Работники не в курсе существования на предприятии механизма информирования	Обращение руководства к работникам	Опрос для оценки доверия к механизму информирования, знаний о нем и связанного с ним опыта
		Напомните в рассылке о ценностях и механизме информирования предприятия
	Сделайте обзор использования механизма	Сделайте обзор того, как механизм до сих пор работал
		Сделайте обзор того, какие уроки предприятие извлекло из работы механизма
Работники не доверяют механизму	Обращение руководства	Заверьте, что предприятие поддерживает информирование и защищает своих работников
	Соблюдайте установленные правила	

Обучение

Работники, выполняющие в механизме информирования определенные роли, должны по возможности проходить соответствующее обучение. Прежде всего нужно сделать так, чтобы они полностью понимали механизм информирования и умели принимать сообщения. В ходе обучения могут рассматриваться следующие темы:

1. Зачем нужны механизмы информирования?
2. Прием сообщений.
3. Обещание конфиденциальности и ее реальное обеспечение.
4. Оценка подозрений.
5. Обратная связь с информатором и предложение ему поддержки.

СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМА

Регулярная переоценка механизма информирования может помочь повышению эффективности инструкций и технических решений. Следует фиксировать количество и тип сообщений, а также результаты расследования по ним, и все эти данные должны для получения максимально независимой оценки направляться, например, совету или аудиторскому комитету предприятия.

Для оценки эффективности механизма информирования подойдут, в частности, следующие индикаторы:

1. соответствие инструкции по информированию и каналов информирования существующему передовому опыту;
2. количество сообщений;
3. доверие к механизму, осведомленность о нем и опыт его задействования работниками;
4. сообщения о преследованиях и
5. число случаев нарушения конфиденциальности.

Количество и содержание сообщений

При оценке эффективности механизма в основном обращается внимание на два таких вопроса:

1. Большое количество сообщений – это хорошо или плохо?
2. Если механизмом пользуются мало, значит ли это, что на предприятии не бывает случаев неправомерного поведения или же речь идет о т. н. культуре замалчивания?

Важность ответов на эти вопросы для предприятия зависит от его размеров, сферы деятельности, рисков, существующих мер контроля, а также того, насколько велика осведомленность работников о механизме информирования и сильно доверие к нему.

РЕКОМЕНДАЦИЯ

Если предприятие использует решение горячей линии, выясните, сколько было на нее звонков и что это были за звонки.

Если предприятие использует решение телефона доверия, уважая конфиденциальность, выясните, с какими вопросами обращались, какая помощь предлагалась.

ПРИМЕР

РЕГИСТР СООБЩЕНИЙ AS EESTI ENERGIA

В AS Eesti Energia записываются все поступившие сообщения о неправомерном поведении, в т. ч. слухи и т. н. разговоры в курилке. Запись в конфиденциальный и открытый только для работников внутреннего контроля регистр вносит тот работник отдела внутреннего контроля, который первым получил сообщение. В регистр заносится содержание сообщения, примечания по расследованию и результат.

Руководству регулярно представляется сводный обзор, в котором описывается, сколько было принято сообщений, от каких подразделений и по каким темам. Более подробно рассматриваются те сообщения, рассмотрение которых потребовало полномасштабного внутреннего расследования. В таком случае руководству поясняется содержание сообщения, что было установлено в ходе внутреннего расследования, и какие были приняты меры для исправления ситуации.

РЕКОМЕНДАЦИЯ

Наибольшую часть сообщений принимают и разрешают, скорее всего, руководители низшего и среднего звена, поэтому ответственному за механизм лицу имеет смысл поинтересоваться его функционированием и у них.

Серьезность случаев неправомерного поведения, а также то, выяснилось ли по результатам расследования, что подозрения имели основание, – значительно важнее просто количества подозрений. Одно подтвердившееся за несколько лет подозрение вполне оправдывает сравнительно скромные расходы на создание и поддержание механизмов информирования. В итоге эти механизмы помогут предприятию избежать крупных убытков и сэкономить.

РЕКОМЕНДАЦИЯ

Если окажется, что сообщения – это в основном связанные с работой жалобы, следует пересмотреть коммуникацию по поводу информирования о неправомерном поведении, потому что работники используют каналы не по назначению.

Если связанные с работой жалобы и сообщения о неправомерном поведении на предприятии рассматривают разные отделы или специалисты, подумайте о создании двух отдельных каналов.

Если все жалобы и сообщения принимает один и тот же отдел или специалист, пусть работники сообщают о своих проблемах, но сделайте так, чтобы, например, на веб-платформе или в опроснике автоответчика присутствовали все вопросы для обоих случаев.

Анализ сообщений

Сведения по количеству и содержанию сообщений позволяют лучше понять **степень осведомленности** и **доверия** работников в связи с механизмом информирования.

Метод оценки осведомленности зависит от размеров и традиций предприятия. Осведомленность можно оценивать, например, следующими инструментами:

1. обсуждением на собрании коллектива,
2. опросами об удовлетворенности,
3. (конфиденциальными) опросами по культуре на рабочем месте.

Вот для примера некоторые вопросы:

1. Сталкивались ли Вы за последние три года с неправомерным поведением на нашем предприятии? Если да, говорили ли Вы кому-нибудь о своих подозрениях и что из этого вышло?
2. Насколько Вы в курсе существующих на предприятии решений по информированию?
3. Насколько велика вероятность того, что, узнав о неправомерном поведении, Вы расскажете о нем своему непосредственному начальнику?
4. С какой долей уверенности Вы можете утверждать, что за обращением к начальству не последует преследований?
5. С какой долей уверенности Вы можете утверждать, что непосредственный начальник отнесется к сообщению серьезно и рассмотрит его корректно?

РЕКОМЕНДАЦИЯ

При составлении вопросов отдавайте предпочтение открытым формулировкам, позволяющим поделиться своими хорошими и плохими мыслями и опытом в связи с механизмом, отношением к информированию и т. п.

РЕКОМЕНДАЦИЯ

Дополнительную информацию по осведомленности персонала и эффективности механизма можно получить и из интервью работника при увольнении.

Исходные данные для оценивания	Инструмент
Соответствие политики информирования на предприятии передовому опыту	Убедитесь, не изменились ли типовые стандарты и рекомендации
Количество сообщений?	Статистика горячей линии (NB! Неиспользование – тоже важный факт)
	Регистр сообщений
	Обзор ситуации от доверенных и принимающих сообщения лиц
Содержание сообщений	Статистика горячей линии (NB! Принцип конфиденциальности)
	Регистр сообщений
	Обзор ситуации от доверенных и принимающих сообщения лиц (NB! Принцип конфиденциальности)
Количество сообщений	Собранная ответственным за механизм лицом статистика

Доверие к механизму, осведомленность о нем и опыт задействования	Опрос работников
Преследования и нарушения принципа конфиденциальности	Опрос работников

В результате промежуточного оценивания может выясниться, что существующему на предприятии решению по информированию еще есть куда развиваться. Например:

1. осведомленность работников низкая:
2. работники не доверяют механизму;
3. работники недостаточно доверяют своему начальству, чтобы делиться своими подозрениями.

В этих случаях организация должна принять соответствующие меры и решить проблемы (см. раздел Повышение информированности).

ИСПОЛЬЗОВАННЫЕ И РЕКОМЕНДУЕМЫЕ МАТЕРИАЛЫ

- Alliance for Integrity (2016) No Excuses! Countering the 10 Most Common Excuses for Corrupt Behavious. A Pocket Guide for Business Practitioners.
- Инспекция по защите данных (2019). Общие инструкции для обработчиков персональных данных.
- Association of Certified Fraud Examiners (2016). Report to the Nations on Occupational Fraud and Abuse.
- British Standards Institute (2008). PAS 1998:2008. Whistleblowing Arrangements. Code of Practice.
- Chartered Secretaries (2010). Guidance Note. A Practical Guide to Good Governance.
- PricewaterhouseCooper (2013). Striking a Balance: Whistleblowing Arrangements as Part of a Speak Up Strategy.
- Public Concern at Work (2007). Rewarding Whistleblowers as Good Citizens. Response to the Home Office Consultation.
- Public Concern at Work (2018). Whistleblowing Best Practice.
- Transparency International (2007). Internal Whistleblowing Mechanisms. Topic Guide. Compiled by the Anti-Corruption Helpdesk.
- Transparency International (2007). The Business Case for Speaking Up. How Internal Reporting Mechanisms Strengthen Private-Sector Organisations.
- Transparency International (2013). International Principles for Whistleblower Legislation.
- Transparency International Nederland (2017). Whistleblowing Frameworks. Assessing Dutch Publicly Listed Companies.
- Transparency International UK (2010). The 2010 UK Bribery Act. Adequate Procedures. Guidance on Good Practice Procedures for Corporate Anti-Bribery Programmes. Checklist.
- Объединение «Эстония без коррупции» (2011). Руководство по предотвращению коррупции для частного сектора.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1. ПРИМЕР ИНСТРУКЦИИ ПО ИНФОРМИРОВАНИЮ

Порядок информирования о неправомерном поведении в AS Tallinna Vesi

1. Введение
2. Наша позиция
3. Наши принципы
4. Как сообщать о подозрении на неправомерное поведение – обязанности работника
5. Что происходит дальше – обязанности предприятия
6. Кого это касается?
7. Пересмотр порядка

1. Введение

Настоящий порядок информирования о неправомерном поведении (далее – Порядок) и Кодекс деловой этики устанавливают этические нормы, действующие в AS Tallinna Vesi и его дочернем предприятии OÜ Watercom (далее в этом документе совместно именуемые AS Tallinna Vesi или Предприятие). Порядок и Кодекс деловой этики AS Tallinna Vesi рассматриваются как единый документ.

Кодекс деловой этики AS Tallinna Vesi размещен на сайте предприятия. Мы в AS Tallinna Vesi гордимся тем, что руководствуемся в своей работе высокими этическими нормами. Они приведены в Кодексе деловой этики, в котором собраны воедино основополагающие принципы нашей бизнес-деятельности. Все работники AS Tallinna Vesi обязаны ознакомиться с этими принципами и знать их. Мы также ожидаем, что наши партнеры будут вести себя в соответствии с высокими этическими стандартами и законом.

Соблюдение в бизнесе принципов честности, справедливости и законности требует от каждого работника определенных шагов в ситуации, когда он видит или предполагает связанное с его работой неправомерное поведение. Мы считаем важным, чтобы при подозрении на неправомерное поведение все наши работники и подрядчики могли доверить имеющиеся у них сведения человеку, который может помочь в сложившейся ситуации. В толковании настоящего Порядка «информирование о неправомерном поведении» означает следующее: работники, клиенты и деловые партнеры Предприятия сообщают о возникших подозрениях на неправомерное поведение, противозаконные действия, бездействие, любое нарушение или проступок (далее совместно – неправомерное поведение) работников или руководства (далее – работники) AS Tallinna Vesi. При этом у информатора нет оснований опасаться преследований, дискриминации, ущемления прав или увольнения.

2. Наша позиция

Цель AS Tallinna Vesi – стать лучшей компанией по оказанию услуг водоснабжения и канализации как в Эстонии, так и в странах Балтии. Безусловно, Предприятие, стремясь к достижению своих бизнес-целей, не идет на компромисс со своими этическими убеждениями.

Даже в самых первоклассных организациях у людей может возникнуть соблазн перейти грань между допустимым и недопустимым поведением. Для того чтобы AS Tallinna Vesi сохраняла и улучшала свою репутацию носителя высоких профессиональных стандартов поведения, чрезвычайно важно, чтобы наши работники знали об активной роли каждого в этом контексте и сообщали о подозрениях на неправомерное поведение, если таковые возникнут.

В настоящем Порядке дается обзор того, как мы побуждаем своих работников сообщать о таких подозрениях.

3. Наши принципы

Неправомерное поведение, о котором работник знает или подозревает, которое могло иметь место или имеет место и на которое распространяется настоящий Порядок, – это:

1. Финансовое или бухгалтерское мошенничество, коррупция, взяточничество или иное ненадлежащее деяние или поведение в финансовой сфере.
2. Недостаточный внутренний контроль на Предприятии или имеющие на нем место крупные аудиторские или бухгалтерские недочеты, которые могут иметь важное или заметное влияние на финансовые результаты Предприятия.
3. Конфликт интересов или неэтичное поведение либо недостаток профессионализма или осмотрительности, например покупка чего-либо у принадлежащего родственнику предприятия или сотрудничество с предприятием, акционером которого лицо является, а также фальсификация данных в коммерческих целях.
4. Использование инсайдерской информации при торговле акциями AS Tallinna Vesi или другого предприятия.
5. Ненадлежащее использование конфиденциальной или деликатной коммерческой информации.
6. Непредоставление внутри Предприятия, или регуляторам Предприятия, или другим соответствующим органам подлежащих предоставлению сведений или уничтожение соответствующих документов.
7. Любого рода преступление или неисполнение юридических обязательств от лица Предприятия.
8. Нарушение условий выданных Предприятием разрешений и лицензий.
9. Создание угрозы или причинение ущерба чьему-либо здоровью и безопасности на работе.
10. Неинформирование о ситуации, в которой ясно, что наша деятельность причинила или может причинить ущерб либо в виде загрязнения, либо иным образом.
11. Несоблюдение порядков, процедур и внутренних правил Предприятия или Кодекса деловой этики.
12. Умышленное сокрытие любой относящейся к вышеприведенным темам информации.
13. Прочие серьезные подозрения.

4. Как сообщать о подозрении на неправомерное поведение – обязанности работника

Работник должен сообщить о своих подозрениях, и чем раньше он это сделает, тем лучше. Все доложенные ситуации рассматриваются, к ним относятся со всей серьезностью и деликатностью.

В первую очередь работник должен сказать о своих подозрениях своему непосредственному начальнику или представителю отдела по работе с персоналом. Мы понимаем, что это деликатные вопросы, поэтому обеспечиваем всем сообщающим о подозрениях полную конфиденциальность и не разглашаем их личности. В случае если рассмотрение ситуации приведет к расследованию, может потребоваться помощь сообщившего о подозрении лица и

его могут попросить дать свидетельские показания. Если информатор соглашается дать показания, ему предлагается консультация и поддержка.

Если работник не хочет рассказывать о подозрении непосредственному начальнику или представителю отдела по работе с персоналом, он может позвонить по специальному номеру для информирования о неправомерном поведении (+372) 786 86 02, который работает 24/7.

Сообщение будет записано, им займется независимый эксперт из Ernst&Young, соблюдая очень высокие требования конфиденциальности.

Кроме того, можно заполнить форму tallinnavesi.ee/vihjeankeet или отправить сообщение по адресу astv@vihja.ee. При заполнении и отправке формы конфиденциальность также обеспечивается – IP-адрес не фиксируется, и работник может быть уверен, что его личность не будет установлена. Информация попадает непосредственно к независимому эксперту Ernst&Young, который изучит ее и примет необходимые меры.

По желанию информатора Ernst&Young сохранит его анонимность при сообщении AS Tallinna Vesi о подозрении на неправомерное поведение, чтобы компания могла предпринять необходимые шаги.

Для максимальной результативности расследования важна точность предоставляемой информации – где и когда случилось, что случилось, кто был с этим связан (люди, должности), как информатор об этом узнал, имеются ли улики и/или свидетели.

Все подозрения, в т. ч. со стороны непосредственного начальства или отдела по работе с персоналом, независимо от того, поступили ли они по горячей линии или через интернет, – изучаются. Если работник сообщил о неправомерном поведении с соблюдением предусмотренной процедуры, мы сделаем всё возможное, чтобы защитить его от возможного давления. В случае если работник сам причастен к неправомерному поведению, AS Tallinna Vesi не может обещать, что не примет в отношении него соответствующих мер, однако факт сообщения об инциденте непременно будет учтен.

AS Tallinna Vesi понимает, что принять решение и сообщить о неправомерном поведении непросто. Если человек взвесил имеющуюся у него информацию и пришел к выводу, что его подозрения обоснованы, ему не нужно бояться, потому что, сообщая, он исполняет свой долг как перед работодателем и коллегами, так и перед клиентами Предприятия.

AS Tallinna Vesi не допускает притеснений и преследований информатора (в т. ч. неофициальных) и принимает меры по защите, если человек сообщил о своих подозрения с добрыми намерениями. Преследования и притеснения Предприятие считает существенными нарушениями трудового договора, которые будут рассмотрены надлежащим образом.

В то же время AS Tallinna Vesi не допускает выдвижения необоснованных, злонамеренных или корыстных обвинений и в таком случае предпринимает соответствующие шаги.

5. Что происходит дальше – обязанности предприятия

После того как сообщение поступило по одному из вышеуказанных каналов, основания для подозрений документируются, принимается решение о дальнейших действиях и ставятся в известность соответствующие руководители, например директор по персоналу, главный юрист и председатель правления или аудиторского комитета (если подозрение касается члена правления).

Все лица, сообщившие о неправомерном поведении и не потребовавшие анонимности, информируются о результатах расследования сразу же, как это станет целесообразным.

6. Кого это касается?

Порядок распространяется на всех работников Предприятия, занятых как на основании постоянного, так и временного договора, а также на подрядчиков.

7. Пересмотр порядка

Все выдвинутые подозрения направляются на рассмотрение аудиторскому комитету Предприятия. Раз в год аудиторский комитет пересматривает Порядок и оценивает его эффективность.

По окончании хозяйственного года топ-менеджмент обязан подписать документ о том, что, по имеющимся у них данным, их подчиненные соблюдают порядок информирования о неправомерном поведении и честны во всех своих делах.

ПРИЛОЖЕНИЕ 2. ПРИМЕР ЧЗВ ПО ИНФОРМИРОВАНИЮ

Часто задаваемые вопросы (ЧЗВ) – Telia Company

ИНФОРМИРОВАНИЕ – ОБЩЕЕ

Есть проблема. Как мне о ней сообщить?

Это можно сделать через решение Speak-Up Line по ссылке www.speakupline.ethicspoint.com.

О чем мне следует сообщать?

Задача Speak-Up Line в том, чтобы люди сообщали о чьем-то некорректном поведении и о других проблемах.

Если есть проблема, не достаточно ли мне будет просто сказать о ней непосредственному начальнику, службе охраны, сообщить в отдел по работе с персоналом, чтобы ею занялись?

Если Вы заметили поведение, которое, на Ваш взгляд, нарушает наши правила, мы советуем Вам об этом сообщить.

В идеале Вы должны обо всех проблемах говорить своему непосредственному начальнику или какому-нибудь члену правления. В то же время мы понимаем, что в некоторых ситуациях такое информирование может доставить Вам неудобства. Вот почему мы пользуемся Speak-Up Line в качестве альтернативного канала информирования.

Почему мне нужно докладывать о том, что мне стало известно?

Мы все имеем право работать в позитивной среде. Этому праву сопутствует и обязанность поступать этично и ставить в известность определенных людей, если Вы заметили, что кто-то поступает неэтично. Вместе прилагая к этому усилия, мы сможем поддерживать здоровый и продуктивный микроклимат. Нарушение правил может негативно влиять на будущее всего предприятия.

Правда что ли, руководство хочет знать о моих проблемах?

Правда! На самом деле, для начальства очень важно, чтобы Вы не молчали. Ведь Вы знаете обо всем хорошем и плохом, что происходит на предприятии. Чем раньше обо всем узнают и

наверху, тем раньше там смогут начать принимать меры, чтобы по возможности уменьшить негативные последствия, связанные с нарушением.

Куда идут эти сообщения? Кто их увидит?

Сообщения напрямую вводятся в защищенный сервер, который находится вне ИТ-среды Telia Company.

Наш провайдер GCS Compliance Services Europe Limited (GCS EU) делает отчеты по сообщениям доступными через систему EthicsPoint только для уполномоченных работников, в задачу которых входит оценивать поступающие сведения и инициировать расследования. Все эти работники обязаны обеспечивать конфиденциальность отчетов.

Не является ли эта система просто вариантом слежки?

Speak-Up Line ориентирована на то, чтобы быть светлой стороной нашей общей философии, и она позволяет нам поддерживать надежную, безопасную и этичную рабочую среду. По поводу этических вопросов всегда можно попросить совета, всегда можно дать хороший совет или сообщить о проблеме. Эффективное общение очень важно для современной компании, и Speak-Up Line – отличный способ его развития.

Мы долго искали самое лучшее решение, которое соответствовало бы требованиям закона, обеспечивая при этом благоприятную коммуникационную среду.

БЕЗОПАСНОСТЬ И КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМИРОВАНИЯ

Насколько я понимаю, отправленное с рабочего компьютера сообщение оставляет на сервере след, по которому можно вычислить все посещаемые мной сайты. Разве нельзя по этому следу установить и мою личность?

EthicsPoint не ведет и не хранит никаких журналов соединений с IP-адресами, поэтому не существует и данных, которые позволили бы соотнести Ваш компьютер с EthicsPoint. Более того, договор с EthicsPoint запрещает устанавливать личность авторов сообщений.

Если Вам неудобно отправлять сообщения с рабочего компьютера, Вы можете войти в защищенную среду Speak-Up Line с любого другого (в интернет-кафе, библиотеке, в гостях и т.д.). Многие так и делают, поскольку, по данным EthicsPoint, менее 12% сообщений поступает в течение рабочего дня.

Могу ли я отправить сообщение из дома, сохранив при этом анонимность?

Сообщение, отправленное из дома, от соседей, через любое интернет-подключение остается защищенным и позволяет сохранить анонимность, если это допускается местными законами. Кроме того, GCS EU не ведет содержащих IP логов интернет-соединений, и, если Вы хотите отправить сообщение, Ваш компьютер невозможно соотнести с GCS EU.

Я боюсь, что после отправки сообщения через GCS EU мою личность раскроют. Как Вы можете гарантировать, что этого не случится?

Целью системы EthicsPoint является защита Вашей анонимности, если она допускается местными законами.

Согласно договору, нам запрещено устанавливать личность информатора. При этом, если Вы хотите сохранить анонимность, Вы должны убедиться, что само содержание сообщения случайно Вас не раскрывает. Например: «У меня в боксе, рядом с Юханом Сидоровым..» или «Целых 33 года...».

Как в сообщении раскрыть свою личность?

Для этого есть специальный раздел.

ПРИМЕРЫ СИТУАЦИЙ

Мне известно, что многие ведут себя неэтично, но со мной это никак не связано. Зачем мне об этом сообщать?

Наше предприятие старается продвигать этичное поведение. Любой неэтичный поступок на любом уровне в конечном итоге наносит ущерб предприятию и вредит всем работникам, включая Вас. Поэтому, если Вам стало известно о нарушении правил или неэтичном поступке, то сообщить об этом – Ваш долг перед собой и коллегами.

У меня нет уверенности в том, что увиденное или услышанное является нарушением правил предприятия или как-то неэтично, но оно мне кажется неправильным. Что делать?

Сообщите. GCS EU поможет Вам составить и передать такое сообщение, чтобы его правильно поняли.

На наш взгляд, лучше, если Вы сообщите о ситуации, в которой не будет выявлено нарушений, чем если что-то неправильное останется без внимания, потому что Вы не были уверены.

А что если мое начальство или другие начальники связаны с нарушением? Не получат ли сообщение они и не начнут ли заметать следы?

Система и процесс информирования работают так, что упомянутые в сообщении стороны не ставятся в известность и не имеют доступа к данной информации.

Что делать, если уже после отправки сообщения мне вспомнилось нечто важное?

Когда Вы отправляете сообщение через сайт, Вы получаете уникальный код, и Вас просят придумать пароль. Через Speak-Up Line Вы можете вернуться к сообщению и уточнить его.

А если Вы сами захотите у меня что-то уточнить?

Когда Вы отправляете сообщение через Speak-Up Line, Вы получаете уникальный код, и Вас просят придумать пароль. С их помощью можно следить за ходом рассмотрения сообщения. После отправки сообщения иногда может пройти несколько дней, пока путь его продвижения не начнет отображаться, и Вам при необходимости сообщат, если для рассмотрения вопроса требуется дополнительная информация. Процесс позволяет разрешать и самые сложные ситуации.

А эти последующие уточнения сообщения – они так же безопасны, как и исходное?

Всё, что отправляется через Speak-Up Line, является конфиденциальным и, если Вы этого хотите и это законно, попадает под требование по обеспечению анонимности.

Мне ведь могут отомстить...

Предприятие категорически запрещает любого рода месть человеку, сообщившему о проблеме. Жалобы, сделанные из лучших побуждений, не связаны для Вас ни с какими санкциями вне зависимости от того, подтвердятся ли подозрения, последует ли принятие мер. Если же Вы считаете, что Вам пытаются мстить, пожалуйста, сообщите об этом, и будет возбуждено расследование.

ПРИЛОЖЕНИЕ 3. ОПРОС ОБ ОСВЕДОМЛЕННОСТИ РАБОТНИКОВ ПО ИНФОРМИРОВАНИЮ О НЕПРАВОМЕРНОМ ПОВЕДЕНИИ

Задача: измерить осведомленность работников о механизме информирования и его эффективности. Для этого выясняется, знают ли работники, куда обращаться, откуда им это известно, обращались ли они, обращают ли они вообще внимание на неправомерное поведение.

Среда: Google Forms, SurveyMonkey или внутренняя сеть предприятия. Подойдут любые платформы, позволяющие экспортировать и в дальнейшем анализировать данные. Если нужно, организация «Эстония без коррупции» окажет помощь в составлении опросника, его дополнении, а также в анализе данных.

Что нужно иметь в виду?

- Перед проведением опроса советуем определить отделы или сектора предприятия, которые могут выделяться, например, по национальному составу, уровню управления и размерам, чтобы отвечающий мог отнести себя к определенной категории. В таком случае можно будет получить представление как о рисках в небольших подразделениях, так и по организации в целом. NB! Если респонденты будут указывать категорию, к которой они относятся, анкету нельзя будет считать полностью анонимной, особенно в небольших организациях.
- В опрос должны быть вовлечены все стороны, которые могут иметь отношение к механизму информирования. То есть, если предприятие принимает сообщения не только от работников, но и от поставщиков, подрядчиков, практикантов или консультантов, то и они должны ответить на вопросы.
- Опрос можно проводить регулярно, например раз в год, чтобы понять главные недостатки механизма, связанные с ним риски и то, насколько хорошо о нем известно.
- Проведение опроса – один из возможных способов донесения информации о существовании механизма.
- При анализе ответов обращайте внимание и на данные, которые на первый взгляд кажутся неважными. Например, если в каком-то подразделении много ответов «не знаю» и т.п., это может указывать не только на то, что там о системе знают мало, но не исключено также, что там плохой микроклимат.

Образец опросника

Ответы на вопросы займут **5–10 минут.** Результаты нужны для оценки мнений работников и их готовности пользоваться механизмом информирования о неправомерном поведении.

Определение

Под неправомерным поведением понимаются действия, которые могут угрожать общественным интересам, связаны с нецелевым или в корыстных целях использованием имеющихся в распоряжении лица ресурсов, в т. ч. для получения льгот. Общественный интерес является интересом общественности в целом и связан с общественными благами, которые не должны использоваться для личного потребления каким-то одним лицом, но должны быть доступны всем. Это – справедливость, равенство, безопасность, природа, культура и т. д.

Неправомерное поведение связано не только со взяточничеством, но и с мошенничеством, фальсификациями и сокрытием, а также со злоупотреблением должностными

полномочиями. В данном случае не имеются в виду прочие связанные с работой или трудовым договором жалобы.

1. **Сталкивались Вы за последние три года на нашем предприятии с неправомерным поведением?** (Выберите один вариант)

- *Да*
    - Вы ответили «да». Говорили ли Вы кому-нибудь о своих подозрениях, и что из этого вышло? (Опишите)
- *Ничего*
- *Не знаю*

2. **Если Вы заподозрите на нашем предприятии неправомерное поведение, знаете ли Вы, кому именно у нас об этом сообщить?** (Выберите один вариант)

- *Да, знаю*
    - Вы ответили «да». Кого Вы имели в виду? (Возможны несколько вариантов)
        - *Непосредственного начальника*
        - *Директора по персоналу*
        - *Внутреннего аудитора*
        - *Кого-то другого (кого?):* ___
            - Пожалуйста, прокомментируйте, откуда Вы знаете, к кому обращаться. (Возможны несколько вариантов)
            - *Это было в пакете для нового работника*
            - *Об этом говорилось на курсах или семинарах*
            - *Об этом пишут в рассылках или в интранете*
            - *Это записано в кодексе этики*
            - *Руководство твердит, что это важно*
            - *Откуда-то еще (откуда?):* ___
- *Не знаю*
    - Вы ответили, что не знаете. Насколько велика вероятность того, что, узнав о неправомерном поведении, Вы расскажете о нем своему непосредственному начальнику? (Выберите один вариант)
    - *Очень велика*
    - *Довольно велика*
    - *Вряд ли*
    - *Точно не непосредственному начальнику*
    - *Не знаю*
- *Не хочу отвечать*

3. **Что, на Ваш взгляд, может помешать сообщению о неправомерном поведении?** (Возможны несколько вариантов)

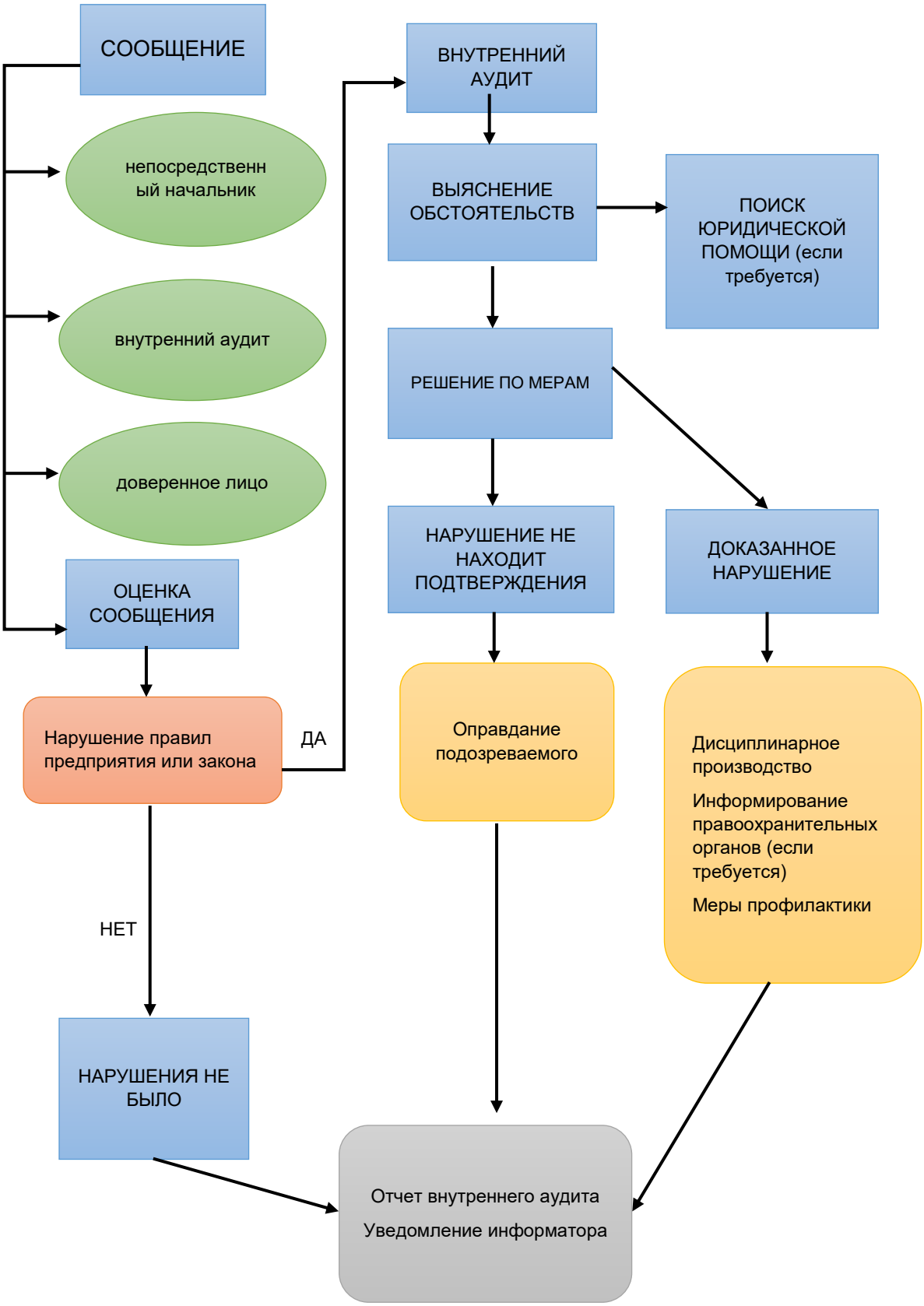
1. *Страх преследования или увольнения*
2. *Опасения за конфиденциальность, что личность информатора будет раскрыта*
3. *Отсутствие информации, к кому обращаться*
4. *Это ни к чему не приведет, поэтому бессмысленно*
5. *Сообщения рассматриваются некорректно*
6. *Не знаю*
7. *Другое (что?):* ___

4. **Насколько уверенно Вы можете утверждать, что непосредственный начальник или принимающее сообщение лицо отнесется к нему серьезно и рассмотрит его корректно?** (Выберите один вариант)

- *Вполне уверенно*
- *Довольно уверенно*
- *Не очень уверенно*
- *Отношение будет несерьезное*
- *Не знаю*

5. **О чем еще нужно было бы спросить?**Напишите обо всех своих дополнительных соображениях. (Комментарий в свободной форме)

ПРИЛОЖЕНИЕ 4. ПРИМЕР ДВИЖЕНИЯ СООБЩЕНИЯ



MTÜ KORRUPTSIOONIVABA EESTI.

TELLISKIVI 60A/3, 10412 TALLINN

INFO@TRANSPARENCY.EE

WWW.TRANSPARENCY.EE

WWW.FB.COM/TRANSPARENCYINTERNATIONALESTONIA