АНДРЕЙ ГЛЕБОВСКИЙ,
заведующий кафедрой экономической безопасности Учебного центра «Информзащита»

Антикоррупционная деятельность компании: некоторые проблемные вопросы получения необходимой информации

В статье «Кадровые аспекты антикоррупционной работы в свете требований ISO37001-2016», опубликованной в № 7 издания «Директор по безопасности» были затронуты некоторые правовые и организационные аспекты реализации основных положений международного стандарта «Системы менеджмента противодействия коррупции» и требований Федерального закона от 25.12.2008 г. № 273 «О противодействии коррупции».

Но, выполняя требования антикоррупционного законодательства по предупреждению ситуации конфликта интересов и личной заинтересованности в сделке, мы рискуем оказаться на той опасной грани, за которой следует нарушение законов, охраняющих неприкосновенность частной жизни и персональных данных физического лица.

Так, из содержания ст. 10 Федерального закона от 25.12.2008 г. № 273 «О противодействии коррупции» следует, что в рамках недопущения возникновения ситуации конфликта интересов, компания должна выявлять личную заинтересованность подлежащего антикоррупционному контролю работника, а именно «возможность получения доходов в виде денег, иного имущества, в том числе имущественных прав, услуг имущественного характера, результатов выполненных работ или каких-либо выгод (преимуществ)».

Прописанная в законе «личная заинтересованность» персонифицируется на следующие категории лиц:

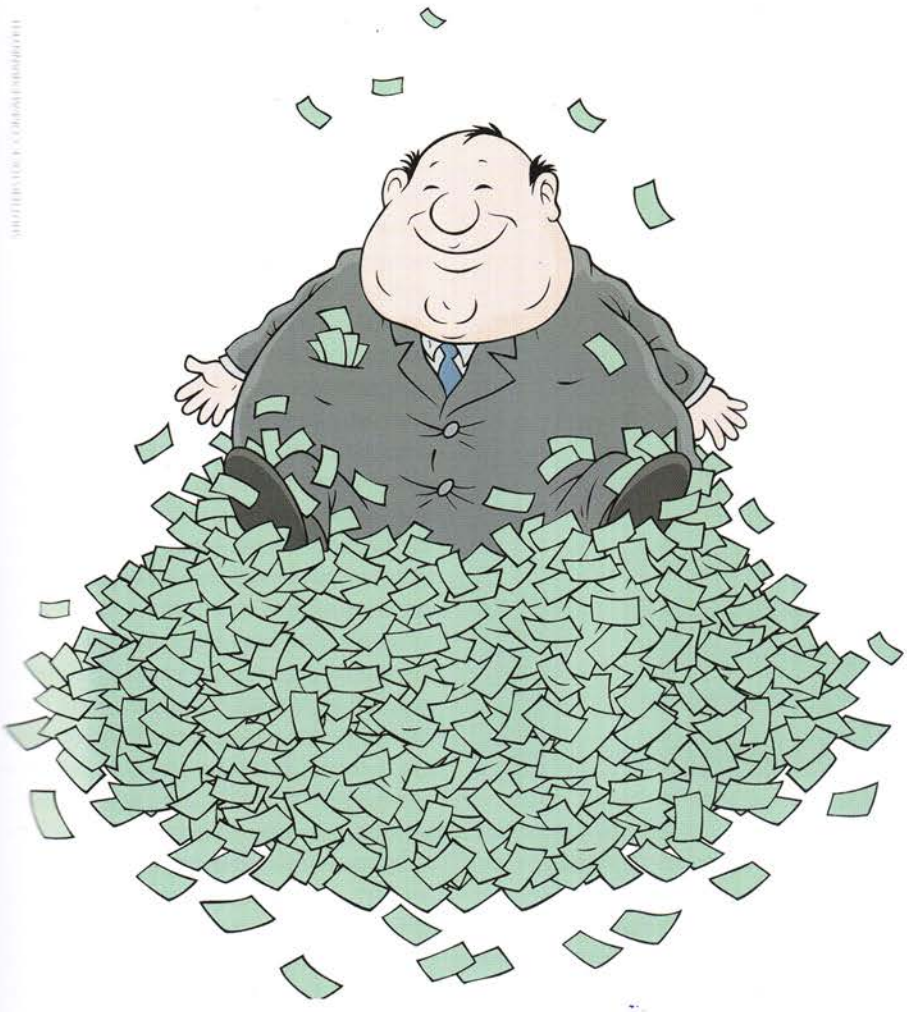
- подлежащие контролю сотрудники государственной компании (а также лица, перечисленные в ч. 1 ст. 81 Федерального закона от 26.12.1995 г. № 208-ФЗ «Об акционерных обществах» и лица, указанные в ч. 1 ст. 45 Федерального закона от 08.02.1998 г. № 14-ФЗ «Об обществах с ограниченной ответственностью»);
- состоящие с ними в близком родстве или свойстве лицами (родители, супруги, дети, братья, сестры, а также братья, сестры, родители, дети супруги и супруги детей);
- граждане или организации, с которыми лица, указанные выше, «связаны имущественными, корпоративными или иными близкими отношениями».

В упоминавшейся статье были даны рекомендации о том, каким образом, не нарушая требований действующего законодательства, выполнить обязанность по выявлению возможной заинтересованности в сделке со стороны родственников (свойственников) подлежащего антикоррупционному контролю сотрудника нашей компании. Но как выполнить это требование в отношении третьей группы – юридических и физических лиц, с которыми наш сотрудник, а также его родственники и свойственники связаны имущественными, корпоративными или иными близкими отношениями?

Представим себе ситуацию: мы беседуем с нашим подлежащим антикоррупционному контролю сотрудником и разъясняем ему, что в соответ-

ствии с законодательством, которое он обязан соблюдать в силу занимаемой коррупционно-емкой должности, на него возложена обязанность проинформировать нас обо всех своих знакомых, с которыми он связан имущественными, корпоративными или иными близкими отношениями. Какова будет реакция сотрудника? Вероятно, законопослушный сотрудник спросит нас: «А в каком законе сформулированы эти понятия? Поясните конкретно, что вы имеете в виду!». И здесь мы, скорее всего, окажемся в затруднении. Если в отношении имущественных и корпоративных взаимосвязей мы можем сказать что-то более-менее внятное, то как быть с «иными близкими отношениями»?

Что это такое? Да и как нам самим определиться, до какого уровня эти «близкие отношения» мы имеем право раскапывать? Даже сама постановка таких вопросов может вызывать естественную реакцию отторжения типа: «Что вы в мою личную жизнь лезете?!». И сотрудник будет прав в своем негодовании. Лично я никогда не решился бы внести в анкету работника графу «Перечислите всех физических лиц, с которыми Вы связаны близкими отношениями». Ведь в бытовом толковании (а законодательного толкования этого словосочетания нет и быть не может) спектр близких отношений между людьми весьма широк: это и друзья детства, и одноклассники, однополчане, бывшие сослуживцы, любовницы и т. д. Повернется ли язык у кого-нибудь из сотрудников контролирующей службы спросить об этом?



Но все эти сомнения мы высказали в отношении нашего работника, на которого в соответствии с ч. 1 ст. 10 Федерального закона от 25.12.2008 г. № 273 «О противодействии коррупции» возложена обязанность «принимать меры по предотвращению и урегулированию конфликта интересов». То есть, в крайнем случае, мы можем ему сказать, что если он не хочет предоставлять нам такую информацию, то он не будет назначен на соответствующую должность, «замещение которой предусматривает обязанность принимать меры по предотвращению и урегулированию конфликта интересов».

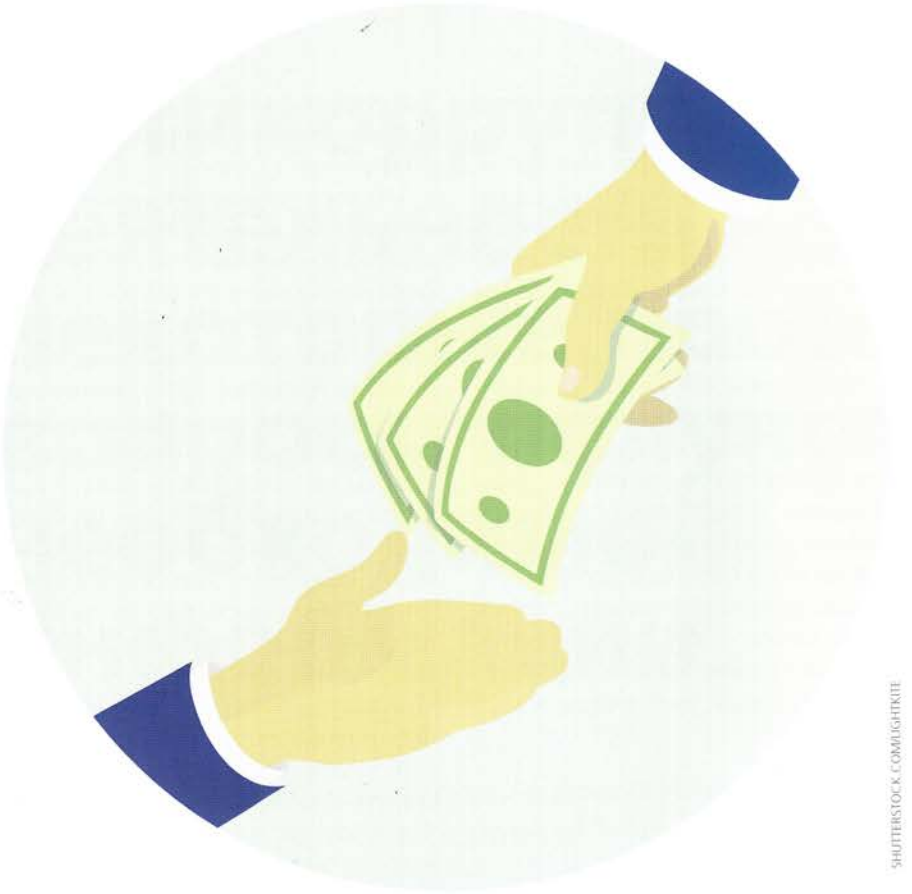
А вот как быть с получением такой информации от другой подконтрольной категории – родственников и свойственников нашего сотрудника? Лично мне ситуация, когда подобные вопросы будут задаваться теще члена совета директоров компании, представляется фантастической, а получение правдивого ответа на него вообще нереально.

Хотя логика законодателя, формулировавшего диспозицию ч. 1 ст. 10 Федерального закона от 25.12.2008 г. № 273 «О противодействии коррупции», понятна и совершенно верна: ведь цель сбора этой информации – исключение возможности возникновения ситуаций, когда конфликт интересов «влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им (нашим работником) должностных (служебных) обязанностей (осуществление полномочий)».

Цель определена правильно, но насколько выполнима задача? Видятся два варианта ее решения:

- проигнорировать это требование закона в силу его изначальной невыполнимости
- попытаться найти средства и методы выполнения требований закона.

Один из вариантов решения проблемы – переложить обязанность антикоррупционного контроля на самого



SHUTTERSTOCK.COM/LIGHTKITE

нашего работника. Сделать это можно, ознакомив его под роспись с положениями ст. 10 упомянутого Федерального закона и строго-настрого предупредив, что если в зоне его служебных интересов появится такой «друг детства» или «сожительница родного брата», то он обязан известить об этом уполномоченный орган компании. Можно не сомневаться, что ни один из сотрудников не откажется дать такую подписку. Но сообщит ли он о возникновении подобной ситуации? Если сотрудник честен и лоялен компании – несомненно. Но антикоррупционные законы пишутся не только и не столько для честных людей. Если наш потенциальный коррупционер замыслит провернуть какую-нибудь махинацию с участием школьного друга и будет знать, что у администрации нет действенных инструментов выявления близких отношений между ними, то наличие такой подписки вряд ли его остановит.

И вот тут логика изложения темы подводит нас к тезису о предписанной нам законодателем обязанности

Один из вариантов решения проблемы – переложить обязанность антикоррупционного контроля на самого сотрудника

контролировать наличие «близких отношений» нашего сотрудника с неопределенным кругом его знакомых. Тема очень деликатная и велика вероятность того, что на посмевшего высказать эту крамольную мысль автора обрушится шквал критики со стороны поборников неотъемлемых прав и свобод гражданина.

Исходя из общих понятий теории риск-менеджмента, нам необходимо сформировать два информационных модуля:

- превентивная информация, т. е. общедоступные сведения обо всех знакомых подлежащего антикоррупционному контролю сотрудника компании;
- ситуационная информация, т. е. подлежащая проверке версия об аффилированности по критерию «наличие близких отношений» руководства появившейся на нашем бизнес-горизонте компании-контрагента подлежащим антикоррупционному контролю сотрудникам нашей компании.

Остановимся подробнее на некоторых особенностях формирования «превентивного» информационного массива. Способ получения информации прост: находим страницу нашего работника в социальных сетях и изучаем через «антикоррупционную» призму круг его общения. Конечно же, весьма условная категория «друг» подконтрольного работника в «Одноклассниках» совсем не означает наличия каких-то близких отношений в смысле соблюдения требований антикоррупционного законодательства. Здесь можно рекомендовать проконтролировать, от кого из десятков или сотен виртуальных «друзей» наш работник получает «подарки» ко дню рождения или по другим датам. Такой «обмен подарками» позволяет предположить наличие между субъектами общения действительно доверительных отношений.

Остается только сожалеть о блокировке Роскомнадзором на территории РФ крупнейшей социальной сети LinkedIn, создававшейся специально для поиска и установления деловых контактов. LinkedIn – это «Одноклассники» для бизнесменов. Там можно было получить информацию о персоналиях и сферах бизнес-активности деловых «друзей» подконтрольного сотрудника. Остается надеяться, что когда владельцы ресурса выполнят

требования Роскомнадзора и сеть снова заработает на территории РФ, работа антикоррупционных подразделений значительно упростится.

И вот здесь автору следует ожидать «помидоров из зала». Дело в том, что некоторые чересчур «законопослушные» представители HR-менеджмента склонны считать такие мероприятия одним из видов оперативно-розыскной деятельности – «снятие информации с технических каналов связи» (п.11 ст. 6 Федерального закона от 12.08.1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»). Но эти упреки из разряда «слышал звон»: этот вид ОРД заключается в негласном съеме информации, передаваемой по сетям электрической связи, компьютерным и иным сетям, путем контроля специальными техническими средствами работы соответствующих систем и устройств, в том числе излучаемых ими электромагнитных и других полей.

Любой человек вправе зайти на открытую страницу пользователя «Одноклассников» и ознакомиться с ней. О какой «негласности» тут можно говорить? Взламывать содержание личной переписки мы не имеем права, а ознакомиться с выложенной в открытый доступ информацией – пожалуйста. Сам автор странички именно для того и выкладывает информацию о себе, чтобы о нем узнало неограниченное число пользователей Интернета. А вот уже какие делать выводы из полученной информации – зависит от профессионализма сотрудников антикоррупционного подразделения. По результатам изучения активности нашего работника в соцсетях мы можем выявить круг контактов и сформировать базу данных потенциальной аффилированности. Эта работа облегчается тем, что некоторые пользователи соцсетей на своей странице указывают места работы или входят в группы, сформированные из сотрудников данной организации.

Обязаны ли мы информировать подлежащего антикоррупционному контролю работника о том, что отслеживали его следы в Интернете? Этот аспект деятельности по обработке персональных данных нашего работника отражен в части 4 ст. 18 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных», согласно которой в подобной ситуации оператор освобождается от обязанности предоставить субъекту персональных данных соответствующие сведения, если персональные данные получены из общедоступного источника. А что может быть доступнее социальной сети?

Еще одно направление – «ситуационный» контроль возможной коррупционной заинтересованности подконтрольного сотрудника применительно к планируемой сделке с контрагентом. Здесь наиболее эффективным методом может быть контроль адресного характера переписки, которую наш сотрудник ведет со своего служебного компьютера. Особое внимание следует уделить контактам, которые активизируются накануне принятия важных (коррупционно-емких) управленческих решений.

Наиболее дискуссионной стороной этого направления сбора информации является вопрос о том, вправе ли работодатель (в лице уполномоченного структурного подразделения) знакомиться с содержанием переписки, которая ведется сотрудником в рабочее время, со своего рабочего места с использованием рабочего компьютера?

Трудовой кодекс РФ (ст. 209 «Основные понятия») гласит, что «рабочее место – место, где работник должен находиться или куда ему необходимо прибыть в связи с его работой и которое прямо или косвенно находится под контролем работодателя».

Отсюда следует, что работодатель вправе (а в определенных случаях и обязан) контролировать, чем занимается работник на своем рабочем месте и как он использует вверенные ему работодателем орудия труда. Запрет водителю в рабочее время халтурить на машине работодателя, контроль со стороны работодателя за его маршрутом с помощью GPS-датчиков и за расходом ГСМ ни у кого не вызывает протестов. Но стоит только обмолвиться о том, что таким же образом должна контролироваться интернет-активность сотрудника в его рабочее время, осуществляемая с его рабочего компьютера, как тут же находится масса яростных оппонентов.

Хотя ситуация с мерой возможного и должного поведения работодателя и работника должна была однозначно проясниться после 12 января 2016 года. В этот день ЕСПЧ принял решение по делу «Б. Барбулеску против Румынии» № 61496/08, в котором разрешил просматривать личную переписку сотрудников и признал увольнение работника в связи с ведением личной переписки с рабочего оборудования в рабочее время законным и не нарушающим личные права сотрудника.

«Желание работодателя убедиться в том, что сотрудники в рабочее время исполняют свои профессиональные обязанности, не лишено смысла», – проявил чувство «тонкого английского юмора» принимавший решение судья ЕСПЧ.

Один из ведущих экспертов по вопросам защиты персональных данных М. Емельянников, подчеркивая неоднозначность решения ЕСПЧ, тем не менее четко определил границы и глубину мониторинга интернет-активности сотрудника. Так, он изложил следующие требования к организации и правовому закреплению подобной деятельности на уровне локальных нормативно-правовых актов:

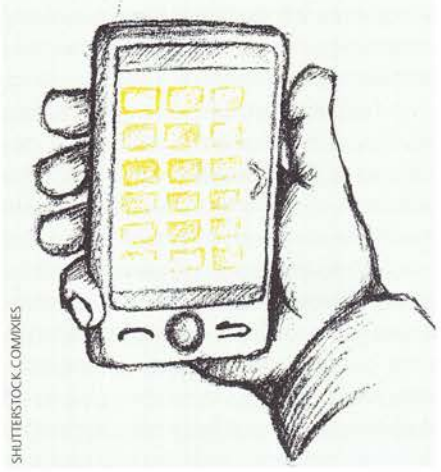
«1. Открытость мониторинга. Его нельзя осуществлять втайне от работника, без ознакомления его под роспись с регламентом проведения контрольных мероприятий.

2. Определение области мониторинга. Очень важно в таком документе определить конкретно, что анализируется работодателем: электронная почта, интернет-мессенджеры, файлы на файл-серверах и в системах хранения данных, приложениях коллективного

ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 25 ДЕКАБРЯ 2008 г. № 273-ФЗ «О ПРОТИВОДЕЙСТВИИ КОРРУПЦИИ» СТ. 10. КОНФЛИКТ ИНТЕРЕСОВ

1. Под конфликтом интересов в настоящем Федеральном законе понимается ситуация, при которой личная заинтересованность (прямая или косвенная) лица, замещающего должность, замещение которой предусматривает обязанность принимать меры по предотвращению и урегулированию конфликта интересов, влияет или может повлиять на надлежащее, объективное и беспристрастное исполнение им должностных (служебных) обязанностей (осуществление полномочий).

2. В части 1 настоящей статьи под личной заинтересованностью понимается возможность получения доходов в виде денег, иного имущества, в том числе имущественных прав, услуг имущественного характера, результатов выполненных работ или каких-либо выгод (преимуществ) лицом, указанным в части 1 настоящей статьи, и (или) состоящими с ним в близком родстве или свойстве лицами (родителями, супругами, детьми, братьями, сестрами, а также братьями, сестрами, родителями, детьми супругов и супругами детей), гражданами или организациями, с которыми лицо, указанное в части 1 настоящей статьи, и (или) лица, состоящие с ним в близком родстве или свойстве, связаны имущественными, корпоративными или иными близкими отношениями.



SHUTTERSTOCK.COM/IXIES

пользования, записи в базах данных, телефонные переговоры и т. п. Такой подход требует документального фиксирования двух ограничений:

- запрета на использование предоставленных работодателем средств хранения, обработки и передачи информации в личных целях
- документально подтверждаемого признания работником того, что он не может рассчитывать на конфиденциальность переписки с рабочего места и с использованием учетных записей, созданных в информационной системе работодателя.

3. Получение согласия работников на мониторинг. …чтобы не создавать конфликтную ситуацию в последующем, отразить такое согласие сразу при приеме на работу – в трудовом договоре.

4. Ограничение возможностей доступа».

http://d-russia.ru/espch-ne-razreshil-rabotodatelyam-chitat-perepisku-rabotnikov-chto-zhe-on-reshil.html

За несколько лет до принятия этого «исторического» решения ЕСПЧ, слушателям линейки курсов корпоративной безопасности Учебного центра «Информзащита» рекомендовалось включить в трудовой договор с работником следующие положения:

- работник ознакомлен и согласен с тем, что компьютерная техника представляется ему Работодателем исключительно для решения служебных задач и не может использоваться в личных целях для хранения, изучения и передачи любой неслужебной информации. Работодатель имеет право контролировать целевой характер использования закрепленной за сотрудником компьютерной техники и выделенного ему интернет-трафика;
- работник ознакомлен и согласен с тем, что корпоративная электронная почта используется им исключительно в служебных целях и Работодатель может контролировать целевое использование корпоративной электронной почты.

Мы обозначили период особо внимательного контроля интернет-активности как «ситуационный» потому что нет смысла проводить эти мероприятия на постоянной основе: у нас для этого не хватит ни сил, ни средств. Условной точкой начала этой работы следует считать совпадение двух аналитических признаков возможной коррупционной ситуации:

- начало проведения преддоговорной работы с определенными признаками возможности актуализации коррупционного риска (объективный фактор);
- проявление «лоббистской» активности подлежащего антикоррупционному контролю сотрудника (субъективный фактор).

На этом этапе неплохие результаты также может дать контроль «абонентской активности» сотрудника. Разумеется, эта работа не имеет ничего общего с оперативно-розыскным мероприятием «прослушивание телефонных переговоров». Поясню, что здесь имеется в виду. В большинстве компаний определенному кругу работников выдаются корпоративные сим-карты и устанавливается определенный стоимостной лимит на телефонные переговоры. Стороной договора по предоставлению услуг связи в этом случае является компания, которая вправе контролировать целевой характер телефонных переговоров своих сотрудников, т. к. компания оплачивает их стоимость оператору мобильной связи.

Логично, что если сотруднику установлен лимит в 2 тыс. руб. в месяц, а он наговорил на 10 тыс., то компания вправе поинтересоваться, кому и по какой необходимости он делал самые длительные и дорогостоящие звонки. Одно дело, если он по служебной необходимости звонил директору компании, находящемуся в загранкомандировке (это будет обоснованное превышение лимита), и совсем другое, если он часами зависал в «Сексе по телефону».

Поэтому слушателям курсов Учебного центра «Информзащита» мы уже давно рекомендуем включать в трудовой договор с сотрудником следующее положение: «работник ознакомлен и

согласен с тем, что предоставляемая ему корпоративная сотовая телефонная связь может использоваться только в служебных целях. Работник ознакомлен и согласен с тем, что целевой характер его разговоров по корпоративной сотовой телефонной связи может контролироваться Работодателем».

Получая такое согласие, работнику следует разъяснить, что никто не будет его прослушивать, но вот запросить у оператора мобильной связи распечатку его переговоров и задать вопрос о том, что за абонент с таким-то номером, которому он сделал 150 звонков за три дня, работодатель имеет право.

Возникает вопрос: как мы без участия нашего работника установим, кому принадлежит телефон наиболее популярного или вызвавшего у нас подозрения его собеседника? Конечно, не прибегая каким-то нелегитимным методам (подкуп сотрудников оператора сотовой связи или правоохранительных органов) мы не можем со стопроцентной достоверностью выяснить личность абонента. Но все же можно попытаться поискать информацию, введя этот номер в поисковую строку «Яндекса» или информационно-аналитической системы («СПАРК» или «Контур.Фокус»). Кроме того, если принимается решение о подключении к антикоррупционному расследованию сотрудников правоохранительных органов, то своевременное предоставление им информации о телефонных контактах наблюдаемого работника существенно повысит эффективность работы оперативников.

При проведении подобных мероприятий немаловажную роль может сыграть тактический аспект использования имеющихся у нас сил и средств. Мы можем затратить массу энергии, пытаясь уловить криминальные признаки коррупционности в массивах повседневной информационной активности подконтрольного сотрудника. Но гораздо эффективнее будут результаты, если мы постараемся «деликатно встревожить» подконтрольное лицо. Общеизвестно, что при пожаре мать бросится спасать ребенка, подпольный миллионер – свою кубышку, а наш потенциальный коррупционер, как правило, не имевший ранее опыта криминального преследования, может утратить бдительность и начать подавать сигналы тревоги своим соучастникам. Вот тут-то и пригодится наш инструментарий контроля интернет – и телефонной активности работника. На практических занятиях мы разбираем со слушателями Учебного центра «Информзащита» подобные ситуации и даем соответствующие рекомендации. К сожалению, предписанные размеры статьи не дают возможности рассказать об этом более подробно.

SHUTTERSTOCK.COM/XIES

Работнику следует разъяснить, что никто не будет его прослушивать, но вот запросить распечатку его переговоров и работодатель имеет право

В заключение хотелось бы обратить внимание читателей на следующее обстоятельство. Мы здесь описали некоторые, наиболее эффективные на наш взгляд методы выявления и контроля коррупционной активности работников нашей компании. Но необходимо учитывать, что речь здесь идет не о рядовых работниках, а о менеджерах среднего и высшего звена. Это изначально придает антикоррупционной деятельности компании несколько своеобразный характер и требует внедрения определенных организационных механизмов, в первую очередь – подчиненность антикоррупционного подразделения высшему органу управления компании. Но это – уже совсем другая история. ●