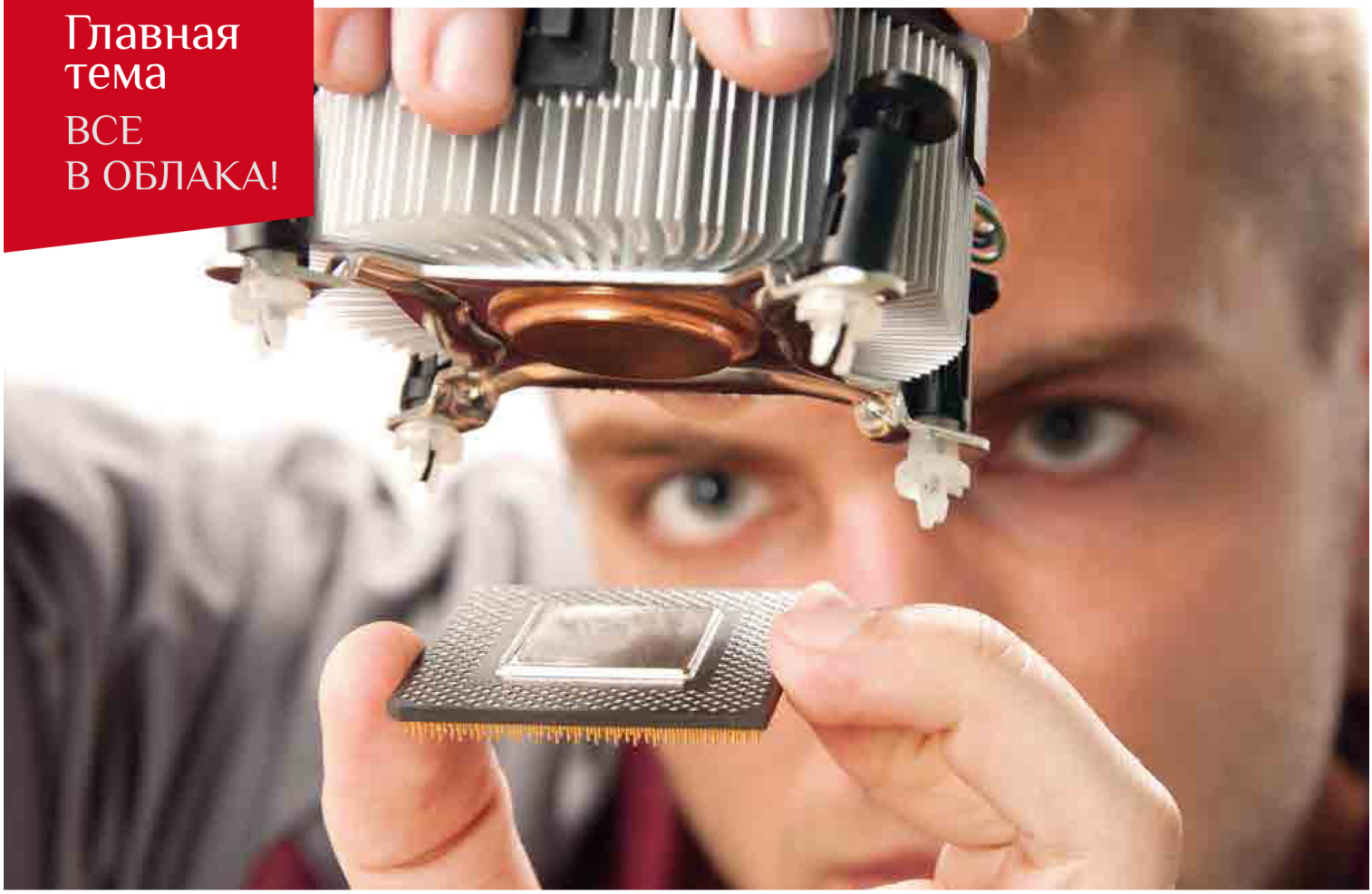
Главная тема
ВСЕ В ОБЛАКА!



Татьяна ПРОЦЕНКО,
управляющий партнер юридической компании «Проценко и партнеры», адвокат

КАК ВЫЯВИТЬ КОРРУПЦИЮ В ИТ-ОТДЕЛЕ

Современный бизнес не может обойтись без активного использования высоких технологий. И если мелкий предприниматель ограничивается одним ИТ-сотрудником, которого легко контролировать, то крупные компании вынуждены нанимать целые отделы. При этом ИТ-специалисты могут не только облегчить работу, но и создать массу проблем, вплоть до непоправимого удара по репутации руководителя или фирмы в целом. При попустительстве руководства сотрудник ИТ-отдела может стать эдаким Богом, которому подвластны практически все электронные процессы организации. Какие коррупционные риски в ИТ-отделе могут ожидать руководство компании и как с ними бороться?

ЕСЛИ ИТ-СЕКТОР ОБХОДИТСЯ «В МИНУС»

При неверно расставленных приоритетах ИТ-сфера — это бездонная бочка для финансовых вложений. Отсутствие же специфических познаний о принципах функционирования ИТ-отдела у руководства создает благоприятную почву для самых разных злоупотреблений. И чем больше размеры компании и подразделения, тем больше различных рисков. В числе самых популярных:

1. Раздувание штата ИТ-отдела без достаточного обоснования.

Выбить пару мест для родственников и друзей для опытного начальника информационного отдела в десяток сотрудников не составит никакого труда, особенно если на месяц погрузить компанию в череду технических сбоев, постоянно сетуя на нехватку рабочих рук для их оперативного устранения.

2. Завышенная стоимость закупки оборудования и программного обеспечения.

Продавать свой товар хотят все, а многие готовы на различные бонусы и вознаграждения за поиск клиента. Что мешает работникам ИТ-отдела договориться с конкретным поставщиком, дав ему важную инсайдерскую информацию для прохождения аукциона, или же «подкрутить» рыночную стоимость оборудования? Практически ничего.

3. Дополнительные объемы работ по обслуживанию и обновлению оборудования.

Ваша компания почти каждый год проводит обновление локальной сети, прокладывая ее с нуля, или каждые два года приобретает новый сервер за несколько миллионов рублей? Возможно, ваши задачи требуют идеальной и стопроцентной надежности всех значимых узлов, но насколько это оправданно?

Главным камнем преткновения при проверке обоснованности тех или иных работ или поставок становится техническая некомпетентность исполнительного органа компании и учредителей. Если ИТ-отдел является обеспечивающим, а деятельность организации напрямую не связана с информационными технологиями, то шансы на то, что топменеджмент в состоянии самостоятельно контролировать происходящее внутри компании, стремятся к нулю.

КОГДА РАСШИРЯТЬ ШТАТ НЕ НУЖНО

В перечисленных случаях тревожными звоночками могут стать подозрительные факты. Например, в случае навязчивого желания отдела увеличить число специалистов руководство должны насторожить следующие обстоятельства:

1. Критические сбои.

После очередного предложения о расширении штата в компании внезапно наступает час икс, связанный с критическими сбоями или отказом информационных систем. Один случай — совпадение, два — тенденция, а три — уже диагноз. И очень плохой.

2. Отсутствуют объективные причины для увеличения числа работников.

Если компания не открывала новых направлений или филиалов, не закупала дополнительное оборудование, не внедряла новые информационные системы, но ИТ-отдел требует дополнительных сотрудников, возможно, стоит сменить руководство этого отдела или основательно проверить, чем же они заняты в рабочее время.

3. Отсутствие нагрузки.

Имеются достоверные сведения от других работников или отделов об отсутствии нагрузки у «информационщиков». Если перед начальством имитировать бурную деятельность легко, то коллеги быстро узнают, что сотрудники ИТ-отдела на рабочем месте заняты посторонними делами, хотя и регулярно напоминают о «высокой нагрузке».

В этом случае желательно обратиться к независимым экспертам, заказав комплексный аудит деятельности компании и целесообразности содержания большого штата специалистов. Аутсорсинг обширного числа задач никто не отменял.

ПЕРВЫЕ ПРИЗНАКИ НЕОБОСНОВАННЫХ РАСХОДОВ

По аналогичному принципу следует действовать и в случае с постоянно растущими расходами на ИТ. Если компания работает стабильно, имеет прибыль и средства для модернизации, то надавить на руководство для опытного (во всех отношениях) айтишника особого труда не составит.

Страшилки о хакерских атаках или отключении всех электронных систем предприятия на сутки или двое с миллионными убытками имеют потрясающий эффект

убедительности, и вот уже учредители готовы согласовать очередное многомиллионное вливание в ИТ-направление компании. В случае несговорчивости следует пара спровоцированных шатдаунов (прекращение работы вычислительной системы), которые непременно будут обоснованы в нужном ключе.

Особое внимание стоит уделять деятельности информационного отдела в следующих случаях:

- свыше 25% сделок или аналогичная величина бюджета достаются одному и тому же контрагенту на протяжении года или более;
- ни руководство, ни учредители ровным счетом ничего не понимают в том, в чем их убеждает ИТ-отдел;
- ИТ-отдел затрудняется обосновать, чем именно выгодны компании те или иные модернизации. Общие фразы не в счет. Цифры, конкретные выгоды — всё это должно лежать в письменном виде в качестве аргументов.

Как же быть? Оставить всё как есть? Разумеется, нет.

В таких ситуациях выход один — нанимать независимых экспертов, чего очень многие компании не желают делать из-за боязни разглашения конфиденциальной информации. Также на подобный шаг не готовы идти и учредители, ссылаясь на коммерческую тайну.

В итоге компания оказывается меж двух огней и чаще всего вынуждена идти на поводу у ИТ-специалистов, предпочитая откупиться от проблем деньгами, нежели впускать в свою работу посторонних лиц.

ВАЖНО: имеет смысл разделить процедуру модернизации на несколько этапов, требуя постоянного отчета от ответственных лиц и контролируя те сферы, в которых менеджмент компании отлично разбирается: ценообразование, порядок выбора контрагента, условия сотрудничества.

Идеально в данной ситуации иметь в составе учредителей или совета директоров специалиста, обладающего достаточными знаниями для надлежащего контроля за ситуацией в ИТ-направлении. Но даже такой человек, если он не является прямо заинтересованным в успешности компании (владельцем пакета акций или доли, инвестором), может быть перекуплен или начать играть в свою пользу.

Однако увеличение затрат на ИТ — меньшая из проблем. В этом случае даже самые недобросовестные айтишники всё же заинтересованы в сохранении экономической стабильности компании и, как следствие, своей «кормушки». Куда хуже обстоят дела, когда у ИТ-отдела возникает иной корыстный интерес.

КТО В РЕАЛЬНОСТИ УПРАВЛЯЕТ ВАШЕЙ КОМПАНИЕЙ?

В век современных технологий реальным властителем ситуации в фирме подчас становится вовсе не генеральный директор, а скромный и тихий системный администратор или же аналогичная по обязанностям команда.

Эти ребята могут практически всё, и это не громкие слова, сказанные ради драматизма. Практика расследования преступлений в сфере ИТ даже в малом и среднем бизнесе знает массу злоупотреблений, например:

1. Сбор конфиденциальной информации о частной жизни сотрудников, руководства.

Часто рядовые работники и даже топ-менеджмент оставляют массу интересного на рабочих станциях, начиная от личных фото и заканчивая пикантной перепиской. При технических и юридических «дырах» в политике безопасности получить доступ к таким данным может обычный системный администратор.

2. Продажа информации конкурентам, содействие рейдерским захватам бизнеса.

Чем больше компьютеризация, тем больше информации о компании в электронном виде. Заинтересованный сотрудник ИТ-отдела без проблем получит сведения о контрагентах, порядке и условиях кредитования, проверках бизнеса и другие важные и интересные определенному кругу лиц данные.

3. Откровенный саботаж или угроза нормальной деятельности фирмы.

Когда сотрудник ИТ-отдела готов уволиться или вступил в прямой конфликт с руководством, то от него можно ожидать любой неприятности — от блокировки работы основных программ до удаления важной информации.

Все эти ситуации становятся возможны из-за недостаточного контроля и попустительства со стороны руководства. Особенно в малом бизнесе, где парочка системных администраторов нередко воспри-