

Управление информационными рисками при переходе юристов из одной компании в другую



Пэт Арчбольд,
руководитель отдела
по рискам в компании IntApp

Последнее время в связи с экономическим кризисом многие компании были вынуждены расстаться с некоторыми сотрудниками. В результате участвовавших увольнений особую актуальность приобрел вопрос о соблюдении определенных требований в области защиты информации. Основная роль при переходе сотрудников и увольнении персонала отводится отделам по управлению рисками и информационным службам компаний.

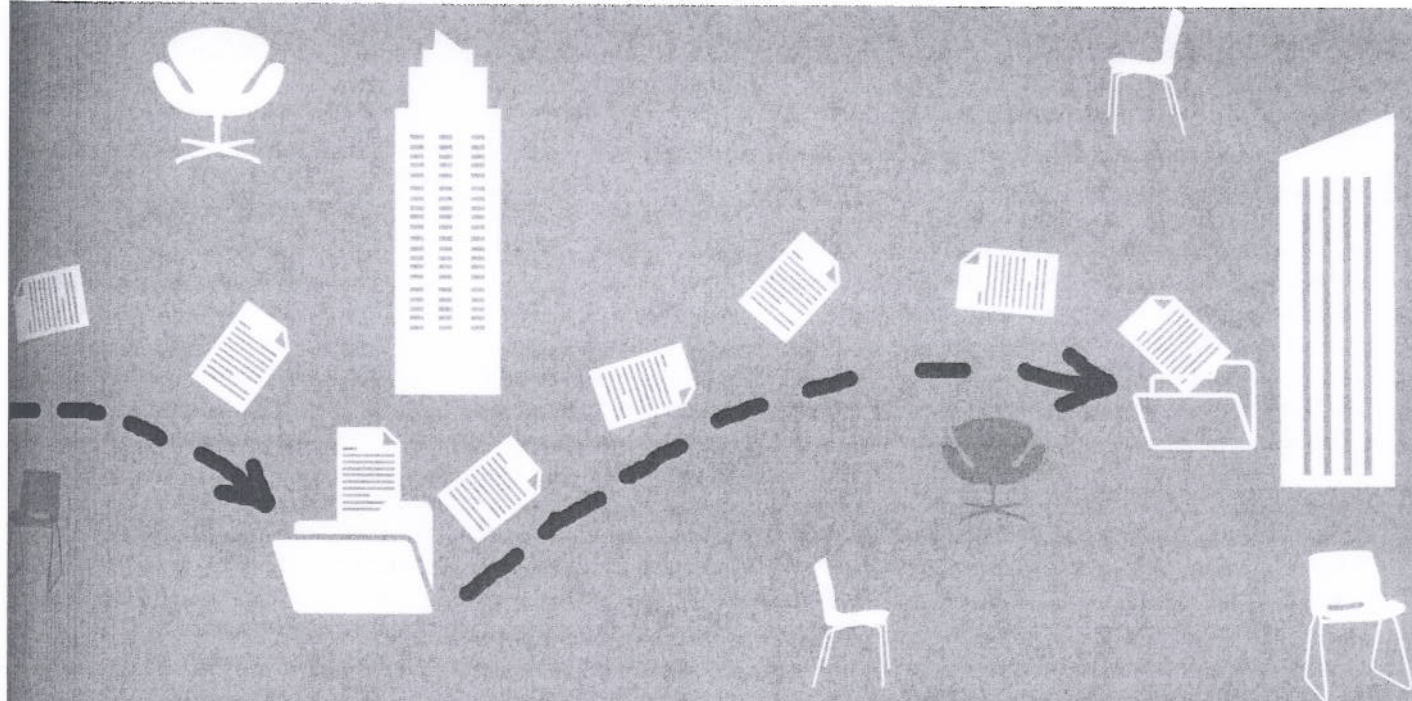
*Перевод с английского М. Исаевой,
компания Threefold*

Настоящая статья была опубликована под названием «Managing information risks with lateral hires and lawyer departures» в журнале «Peer to Peer» в марте 2010 г., издаваемом ILTA (международной организацией, занимающейся предоставлением информации об использовании современных технологий в юридической профессии), и перепечатывается с их разрешения. Более подробную информацию об ILTA можно найти на сайте www.iltanet.org

Откройте дверь, опустите занавес

Общепринятая на сегодняшний день практика перехода юристов из одной фирмы в другую чревата возникновением конфликтов интересов. Для их урегулирования весьма эффективным является механизм так называемого «этического занавеса» (ethical screen). В некоторых странах для его установки необходимо получить от клиентов (в том числе бывших) согласие и письменный отказ от каких бы то ни было претензий в дальнейшем. Однако в США, все в большем числе штатов, этого не требуется.

Готовность юридических компаний к возможности предъявления им иска противоположной стороны о дисквалификации в связи с нарушением правил конфиденциальности информации становится вопросом жизненной необходимости, ведь выиграть дело в суде можно только в том случае, если удастся доказать осуществление всех надлежащих внутренних



процедур и использование эффективных механизмов для ограничения доступа к внутренней релевантной информации.

Современная защита от этических конфликтов

Изначально «этические занавесы» являлись главным образом инструментами внутренней политики. Для обеспечения собственных профессиональных обязательств фирмы издавали меморандумы, во избежание ненадлежащей передачи информации призывали сотрудников к личной предусмотрительности, а в качестве меры предотвращения случайного раскрытия информации обозначали ограниченный доступ к ней путем маркирования «красными стикерами». Современные технологии вытеснили такую практику. Сейчас почти вся информация создается и хранится на электронных носителях, а это предоставляет заинтересованным лицам определенные возможности доступа к клиентской и внутренней информации компании.

В связи с этим отраслевые стандарты в сфере конфиденциальности претерпевают изменения. На смену прежним способам обеспечения безопасности пришли автоматическое уведомление и автоматическая отчетность. Такие нововведения обусловлены настоятельными требованиями клиентов по поводу использования фирмой документированных и подлежащих проверке процедур «этического занавеса» в ответ на предложение подписать отказ от возможных претензий. Этому также способствует обновление правил профессионального поведения юридического сообщества и формирование более жесткой и однозначной судебной практики.

Недостаточная защита приводит к поражению

К сожалению, известны примеры и неудачного использования механизма «этического занавеса». Так, в

Ethical screen

Речь идет о процедурах и правилах, с помощью которых можно предотвратить потенциальный конфликт, связанный с переходом сотрудника из одной фирмы в другую. Например, недавно пришедший в компанию новый юрист ранее представлял интересы клиента А против клиента В. Последний, как выяснилось, является клиентом фирмы, в которую пришел работать юрист, и теперь этот сотрудник может использовать полученную на предыдущем месте работы информацию в ущерб своему бывшему клиенту А. Механизм «этического занавеса» в большинстве случаев базируется на Model Rules of Professional Conduct. Для отслеживания потенциальных конфликтов создаются специальные программные продукты и базы данных.

2009 г. одна из фирм, входящих в рейтинг AmLaw 200 (ежегодный рейтинг журнала The American Lawyer), была дисквалифицирована за его несвоевременное введение. В ходе разбирательства судья указал на то, что задержка с установлением «занавеса» стала решающим фактором для признания его неэффектив-

Сейчас практически вся информация создается и хранится на электронных носителях, а это предоставляет заинтересованным лицам определенные возможности доступа к клиентской и внутренней информации компании

ности, а для сравнения привел примеры из судебной практики, подтверждающие достаточность таких превентивных мер в случае их своевременного принятия.

В другом решении суд отклонил иск о дисквалификации компании на основании достаточности принятых ею мер (установления «занавеса»). В то же время компании были даны указания по имплементации

Довольно часто при переходе в другую фирму на аналогичную должность юристы удаляют свои рабочие файлы, поскольку полностью уверены в том, что их клиенты уйдут вслед за ними

дополнительных механизмов защиты посредством расширения контроля над безопасностью информации, а именно программы учета затраченного времени и регулярной рассылки внутренних напоминаний в связи с установлением «занавеса».

Необходимость установления «занавеса»

Как показывает практика, угроза дисквалификации юридических компаний возникает при несвоевременном установлении ими «этического занавеса», недостаточном контроле над доступом к информации и несовершенной системе внутренних уведомлений, причем для признания «занавеса» неэффективным не требуется доказательства факта раскрытия информации. Сама возможность получения доступа или включения в список получателей ограниченной информации (даже по случайности) уже вызывает сомнение в его надежности, особенно когда конкурирующие фирмы применяют слишком жесткие меры защиты.

Рост количества судебных дел, связанных с установлением «этического занавеса», положил конец практике работы сотрудников под «честное слово» и использованию «красных стикеров». Сейчас необходимо своевременно принимать эффективные меры, на которые можно будет сослаться в ответ на запрос клиента или в случае предъявления судебного иска.

Меняются нормы, меняются ожидания

Стандарты юридических компаний в области установления «этического занавеса» формируются не только на основе судебной практики, но и с развитием профессиональных норм, обусловленных интенсивностью перехода юристов из одной фирмы в другую. Американская ассоциация адвокатов (АВА) недавно обновила свой модельный регламент, приняв положение, позволяющее компаниям устанавливать «занавес» без согласия клиента, и введя дополнительные требования к обеспечению исполнения, уведомлениям и отслеживанию.

В других странах действуют сходные, иногда более строгие правила. Например, в Соединенном Королевстве Великобритании в качестве «занавеса» применяется такой способ обеспечения конфиденциальности информации, как «электронный барьер от распространения информации».

Канадская ассоциация адвокатов (СВА), принимая в 2008 г. довольно щадящий регламент по установле-

нию «занавеса», подчеркнула важность используемой технологии: применение современных программ по защите конфиденциальности позволяет ограничить доступ к электронным документам, предоставляя его только тем, кто имеет для этого специальное разрешение. В основу таких программ может быть положен учет времени, затраченного на работу по конкретному проекту уполномоченными на то лицами. Компьютеризированные системы мониторинга и безопасности вселяют надежду на обеспечение эффективной защиты информации.

Тенденции по управлению вопросами конфиденциальности

К сожалению, некоторые компании все еще не используют соответствующие механизмы для обеспечения конфиденциальности информации и тем самым подвергают себя серьезным рискам. Некоторые предпочитают рассылать меморандумы и вручную настраивать базовые механизмы безопасности для документов, игнорируя инструменты управления данными, уведомления и постоянного слежения, поддержки и отчетности.

Конечно, ни одна компания не хочет предстать перед клиентами, судом, прессой и регулируемыми органами виновной в раскрытии конфиденциальных данных, поэтому большинство из них делают все возможное для укрепления политики, стандартов и механизмов защиты информации. С учетом значительности рисков, от которых не застрахована ни одна компания, подобные усилия следует признать весьма целесообразными.

Стремление следовать профессиональным стандартам в области обеспечения конфиденциальности порой сдерживается весьма обременительными требованиями. Ручное управление не позволяет достичь таких результатов, как при использовании автоматических механизмов. Организации, желающие обеспечить самую надежную защиту от возможных рисков, применяют наиболее совершенные технологические решения по обеспечению конфиденциальности информации. Согласно обзору рисков для юридических фирм за 2009 г., подавляющее большинство компаний, входящих в рейтинг NLJ 250 (ежегодный рейтинг журнала The National Law Journal), ведут специально разработанную внутреннюю политику или осуществляют электронный контроль данных, требующих применения процедуры «этического занавеса» либо каких-то других правил обеспечения конфиденциальности.

Управление рисками в случае увольнения сотрудников-юристов

Для юридических компаний увольнение сотрудников может быть сопряжено со значительными потерями – от прямых убытков, связанных с уходом клиентов, до

Риски утечки компьютерной информации

До начала повсеместного использования технологий для создания, распространения и управления результатами работы и клиентской информацией ненадлежащее перемещение информации сложно было не заметить. Доминирующим носителем была бумага, что, безусловно, облегчало отслеживание несанкционированного перемещения документов. Забрать с собой большое количество материалов было непросто: приходилось сначала подбирать нужные дела, затем копировать их и выносить или даже вывозить на специальных тележках, для чего, как правило, требовалась помощь сотрудников архива или другого вспомогательного персонала.

В наши дни клиентскую и внутреннюю информацию компании можно легко и быстро скопировать в большом объеме и тайно переместить. Такие средства, как электронная почта, системы управления документами, программы поиска и управления знаниями, создают неограниченные возможности в плане производительности и обмена информацией. Простота доступа к сведениям и ограниченность контроля позволяют поместить аналог целой библиотеки на один маленький диск, который так легко незаметно вынести за пределы компании. На маленьком iPod-е может быть перенесено огромное количество информации, охраняемой законом об интеллектуальной собственности. Однако за подобные привилегии можно серьезно поплатиться.

косвенных, выражающихся в утрате взаимоотношений и знаний. Порой риски, возникающие при увольнении юристов, превалируют над потерей клиентов. В связи с этим в преддверии ухода сотрудника из компании необходимо определить, какие бланки, файлы и сведения о клиентах «уйдут» вместе с ним.

Риски, связанные с конкуренцией и недобросовестной практикой юридических фирм, существенно возрастают при перемещении клиентских данных до предоставления на это официального согласия, а также в том случае, если уволившиеся юристы берут с собой проекты документов, подготовленных для клиентов, остающихся с фирмой, или из информационной библиотеки знаний компании. Довольно часто при переходе в другую фирму на аналогичную должность юристы удаляют свои рабочие файлы, поскольку полностью уверены в том, что их клиенты уйдут вслед за ними. Однако с учетом рисков, связанных с обеспечением конфиденциальности, управлением данными и прочей информацией, даже малейшее нарушение в управлении информационным потоком может иметь серьезные последствия как для клиентов, так и для компаний.

Порой фирмы, вкладывающие существенные средства в создание превосходного программного продукта для рабочих процессов и подборку прецедентов, даже не подозревают, что информация уходит от них к конкурентам. Такое часто происходит в результате неуправляемого перемещения информации. Если поток сведений обходит систему архивирования, то

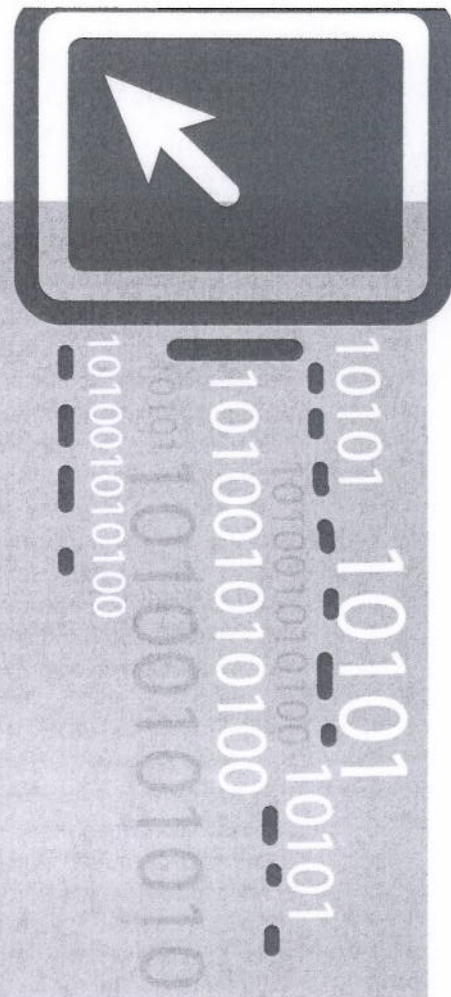
подлежащие уничтожению документы сохраняются, и в итоге конфиденциальные данные, которые клиент считал уничтоженными, всплывают в ходе судебного разбирательства.

Практика вразрез правил

Внутренние правила многих компаний прямо запрещают сотрудникам при уходе забирать с собой без согласования какую-либо информацию. Однако на практике выясняется, что одни не были осведомлены об этом, другие не считали подобные нормы применимыми к себе, иные просто надеялись безнаказанно увести с собой клиентов. Последнее обстоятельство заставляет учитывать, что файлы клиентов являются их собственностью, а их несанкционированное перемещение создает угрозу юридического преследования со стороны клиентов как в отношении той фирмы, откуда сотрудник увольняется, так и той, в которую он устраивается. Таким образом, для обеспечения соблюдения профессиональных и этических обязательств компании жизненно необходимо отслеживать, как увольняющиеся сотрудники обращаются с конфиденциальной информацией.

Устранение рисков, связанных с утечкой информации

Учитывая риски, связанные с утечкой клиентской информации, а также внутренней информации компании, фирмы должны тщательно продумывать меры защиты.



Начинать всегда следует с оценки действующих норм и процедур. Весьма полезно собрать и проанализировать мнение сотрудников ключевых отделов: информационного, архивного, персонала, управления рисками. Это позволит выработать основу для внутреннего обучения и проведения тренингов.

Иногда недозволенное перемещение сведений происходит по ошибке или из-за недопонимания сотрудников. Использование механизмов уведомления и управления вопросами внутренней стратегии обеспечит понимание сотрудниками компании правил и стандартов обращения с конфиденциальной информацией. Также полезно проводить тренинги «невольных сообщников» – сотрудников службы технической поддержки, архивов и прочих для выработки у них умения распознавать подозрительные признаки необычной деятельности. В ходе таких тренингов вспомогательные сотрудники обучаются четкому иерархическому поведению, что освобождает их от необходимости наблюдения за юристами. К примеру, требование юриста к службе технической поддержки собрать и заархивировать историю электронной почты может служить основанием для проведения внешней проверки.

Важная роль в обеспечении безопасности информации отводится применению различных технологий. Например, отследить нарушителя можно посредством использования инструментов, позволяющих присылать уведомления о тех действиях пользователя электронной библиотеки, которые выходят за рамки обычных. Сигналом к проверке также может стать большое количество просматриваемых юристом базовых документов. Система подобных уведомлений устанавливается в зависимости от общих предельных значений либо для наблюдения за конкретным офисом, где ожидаются или планируются увольнения. Наличие системы уведомления о нестандартных действиях пользователя создает возможность раннего реагирования. В результате использования системы уведомлений многим фирмам удалось предотвратить нежелательное увольнение своих юристов. Отдельно следует отметить относительную лояльность такого подхода в силу его открытости для сотрудников компании.

Итак, с приходом или уходом очередного юриста компания должна принять все необходимые меры по соблюдению требований в области управления рисками, связанными с доступом к информации и возможностью ее перемещения. Создав предпосылки для увеличения числа ошибок и недочетов в работе с конфиденциальной информацией, развитие информационных технологий в то же время предоставляет компаниям все новые возможности по ее защите.

За последние годы выработаны достаточно надежные механизмы по обеспечению конфиденциальности информации. Многие компании стали тщательнее

подходить к процедурам внутреннего контроля, тем самым ужесточая профессиональные стандарты юридического сообщества. Одновременно повышаются требования клиентов, страховых компаний и судей. Жизненно важной для юридических фирм становится разработка информационным отделом и отделом compliance стратегии защиты, отвечающей современным вызовам, ведь объяснять суду или клиенту, почему компанией не были приняты меры по предотвращению утечки информации, весьма проблематично.



Комментарий Анны-Стефании Чепик, партнера PwC Legal CIS

Как в России регулируются конфликты, возникающие в связи с неправомерным распространением конфиденциальной информации клиента при переходе юриста из одной фирмы в другую?

Для России вопрос защиты конфиденциальной информации клиента при переходе юриста из одной фирмы в другую является очень болезненным. Дело в том, что никакого специального регулирования именно в отношении юридических фирм в части защиты конфиденциальной информации клиентов в российском законодательстве нет. У нас есть лишь общие нормы Федерального закона «О коммерческой тайне», который предусматривает возможность введения режима коммерческой тайны фирмой, и положения Трудового кодекса, которые позволяют



предусмотреть обязанность юриста не распространять и не использовать информацию, составляющую коммерческую тайну. Фактически защитить коммерческую тайну (в том числе конфиденциальную информацию третьего лица – клиента) в России очень тяжело: помимо административно тяжеловесного режима коммерческой тайны практически полностью отсутствует положительная судебная практика. В силу того, что суды склонны очень формально подходить к оценке доказательств, подтверждающих неправомерное раскрытие и использование конфиденциальной информации, доказать незаконное использование коммерческой тайны в суде практически невозможно. Поэтому как компании не могут защитить свои интересы при неправомерном использовании информации бывшими работниками, так и их клиенты не могут доказать неправомерное раскрытие информации и возместить причиненные убытки. В результате клиенты юридических фирм не могут получить адекватной правовой защиты в случае несанкционированного раскрытия конфиденциальной информации при переходе юристов из одной компании в другую. Однако помимо правовых

аспектов, есть репутационные, и, конечно, юридические фирмы борются за сохранение и обеспечение конфиденциальной информации клиентов, боясь не потенциальных судебных исков, а потери клиентов. Надо отметить, что и многие юристы следуют неписаным правилам профессиональной этики, понимая, что, помимо ответственности, есть и личная репутация.

Известны ли российской судебной практике случаи рассмотрения дел по ненадлежащему управлению информацией сотрудниками юридических фирм?

Мне такие случаи неизвестны. Судебных споров по защите конфиденциальной информации в России, в принципе, крайне мало, и имеющиеся судебные решения, к сожалению, говорят не в пользу собственников конфиденциальной информации.

Как Вы считаете, являются ли механизмы по защите информации, принятые на Западе, эффективными?

Сложно дать правовую оценку тому, что ни разу не проверил на практике.

Безусловно, у клиентов должны быть реальные механизмы возмещения вреда в случае неправомерного распространения или использования конфиденциальной информации и должны быть эффективные меры контроля. Другими словами, система должна позволять привлекать к ответственности юридические фирмы (и юристов как работников) уже тогда, когда создалась угроза раскрытия информации, а не только когда информация уже была раскрыта. Ценность конфиденциальной информации связана именно с ее неизвестностью третьим лицам: если это условие нарушается, конфиденциальная информация перестает быть таковой и ее ценность исчезает. Поэтому при защите конфиденциальной информации очень важно именно не допустить ее неправомерного раскрытия. К сожалению, российская правовая система пока не предусматривает какого-либо механизма контроля со стороны клиентов (собственников конфиденциальной информации) и адекватных мер ответственности в отношении юридических фирм в случае создания угрозы распространения конфиденциальной информации. ¹⁵