№ 35
СЕНТЯБРЬ 2016
ЭЖ ЮРИСТ

ЗАЩИТА ИНФОРМАЦИИ:

СПОСОБЫ ЗАЩИТЫ

Максим АЛИ,
юрист практики
по интеллектуальной собственности /
информационным технологиям,
Адвокатское бюро «Качкин и Партнеры»,
г. Санкт-Петербург

С правовой точки зрения можно выделить следующие основные способы защиты информации, актуальные для юридических компаний и иных лиц.

1 Гражданско-правовой договор о неразглашении конфиденциальной информации (non-disclosure agreement – NDA). Стороны могут заключить такой договор, руководствуясь принципом свободы договора (п. 2 ст. 421 ГК РФ) и тем, что информация сама по себе является объектом гражданских правоотношений (п. 1 ст. 5 Федерального закона от 27.07.2006 «Об информации, информационных технологиях и о защите информации»). Особенностью такого способа защиты является, во-первых, относительной характер ее действия (ответственность несет только контрагент), а, во-вторых, относительная свобода сторон в определении санкций за неисполнение договора (наиболее распространенным вариантом является неустойка, которая, однако, может быть снижена в порядке ст. 333 ГК РФ).

2 Введение в компании режима коммерческой тайны. Данный режим распространяется только на сведения, имеющие потенциальную или действительную коммерческую ценность (п. 2 ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне»). Преимуществами данного способа защиты являются, во-первых, возможность увольнения работника за разглашение составляющих коммерческую тайну сведений (подп. «в» п. 6 ст. 81 ТК РФ), а также возможность применения уголовной ответственности за их незаконное собирание, разглашение или использование (ст. 183 УК РФ). К недостаткам следует отнести излишнюю формализованность режима: для признания факта его введения компании необходимо принять все меры из п. 1 ст. 10 Закона № 98-ФЗ, в том числе нанести грифы «коммерческая тайна», определить перечень секретной информации, определить порядок обращения с ней и принять меры по контролю за таким обращением, вести учет лиц, допущенных к указанным сведениям. Проще говоря, предусмотренный Законом порядок введения режима коммерческой тайны является весьма забюрократизированным, что особенно осложняет использование такого механизма небольшими компаниями. Кроме того, законодательное регулирование в этой области порой противоречиво: к примеру, незаконное собирание сведений, составляющих коммерческую тайну, не может быть основанием для увольнения работника согласно ст. 81 ТК РФ, однако является преступлением в силу ч. 1 ст. 183 УК РФ.

3 Охрана информации, составляющей адвокатскую тайну. К такой информации относится крайне широкий круг сведений, поскольку ключевой критерий их отнесения – связь таких сведений с оказанием адвокатом юридической помощи доверителю (п. 1 ст. 8 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»). Учитывая, что обязанность адвокатов по сохранению конфиденциальности полученной ими информации следует из Закона и не связана с соблюдением разного рода формальностей (как в случае с коммерческой тайной), доверитель автоматически находится в более выгодном положении, чем заказчик юридических услуг в отношениях с юридической компанией, созданной в иной форме. В перспективе доверитель может требовать возбуждения дисциплинарного производства в отношении адвоката, а также применения гражданско-правовых мер ответственности (например, возмещения убытков или компенсации морального вреда). Однако режим адвокатской тайны дает некоторые преимущества и самому адвокатскому образованию: разглашение таких сведений является основанием для увольнения сотрудников адвокатского образования, не являющихся адвокатами, что следует из п. 10 Кодекса профессиональной этики адвоката и уже упомянутой ст. 81 ТК РФ. Что интересно, разглашение адвокатской тайны не является уголовно-наказуемым деянием, поэтому публично-правовая ответственность адвоката будет ограничиваться штрафом до 5000 руб., предусмотренным ст. 13.14 Кодекса РФ об административных правонарушениях.

Важно также понимать, что юридическая защита информации не может быть эффективной без механизма фиксации нарушений порядка обращения с конфиденциальными сведениями, который обеспечит формирование доказательственной базы на будущее. Ввиду того что обращение в правоохранительные органы на практике не всегда будет плодотворным, организациям, претендующим на высокий уровень информационной безопасности, надо самостоятельно налаживать процессы по отслеживанию правонарушений и дальнейшей работе с ними в порядке гражданского, административного или уголовного производства.

Следует помнить и то, что информационная безопасность является комплексной задачей, достижение которой возможно лишь при использовании разнонаправленных мер защиты информации, охватывающих не только правовые, но и организационно-технические аспекты охраны конфиденциальности.

КНУТ И ПРЯНИК

Эрнест АСЛАНЯН,
частный детектив, старший преподаватель
Института бизнеса и права Москвы,
г. Москва

В ситуации с утечками конфиденциальной информации различного рода (прежде всего финансового) необходимо понимать несколько ключевых моментов.

Во-первых, это большая политика. Такие большие утечки не рождаются из ничего, не случаются на ровном месте. Просто есть определенные группы, которым на данный момент это выгодно. Здесь с вероятностью в 100% корни растут из спецслужб: без активных действий разведки такое попросту невозможно. Скорее всего, утечка из Mossack Fonseca была спланирована заранее и осуществлена силами западных разведок (прежде всего Центрального разведывательного управления и MI6). А раз это большая политика и деятельность сильнейших разведок мира, защититься практически невозможно.

Во-вторых, как говорил далеко не самый глупый глава советского государства, если у случайности есть политические последствия, значит, ищите у этой случайности фамилию, имя и отчество. В данном случае кадры решают все, ведь информацию на сторону всегда передают вполне конкретные люди, сотрудники таких компаний. Если не хотите утечек строго конфиденциальной информации о своих клиентах, подбирайте персонал с тройной осторожностью и выстраивайте мощную систему защиты от распространения инсайдерской информации. Лучше всего не вводить ничем не подкрепленные запреты на передачу и использование инсайда, но грамотно использовать кнут и пряник: доплачивать сотрудникам за молчание и предусмотреть жесткие механизмы наказания за любые утечки. Когда на кону не только деловая репутация, но и само существование фирмы, с такими вопросами необходимо разбираться жестко.

В-третьих, офшоры понемногу теряют свою популярность: о них уже написали сотни и тысячи статей, десятки книг, а Россия по решению Президента В. Путина начала активную деофшоризацию. В рамках этой политики нужно четко понимать, что контроль за налоговыми гаванями в России усилился в разы, и заниматься этим теперь не просто опасно, но и незаконно. Однако те же спецслужбы не забывают, что офшоры – мощный инструмент глобальной политики. Поэтому в экстренных случаях и вытаскивают подобную информацию. Чтобы не попасть в такое затруднительное положение, лучше не иметь дела со скользкими темами вроде темы офшоров. А фирмы, которые берутся за подобное, изначально должны понимать, что риски крайне высоки и вероятность попасть на первые полосы изданий в неспокойной политической обстановке стремится к бесконечности.

СОВЕТЫ И РЕКОМЕНДАЦИИ

Кирилл БЕЛЬСКИЙ,
старший партнер, руководитель практики
разрешения споров,
Адвокатское бюро «Коблев и партнеры»,
г. Москва

Еще несколько лет назад пресса пестрила сообщениями о взломе телефонов и почтовых ящиков звезд шоу-бизнеса.

Сегодня риски кибератак вынуждены принимать во внимание абсолютно все: частные пользователи, малые бизнесы, транснациональные корпорации, органы исполнительной власти и силовые структуры.

Особенный интерес у хакеров в последнее время вызывают юридические и аудиторские фирмы: их базы данных хранят терабайты ценнейшей информации о клиентах. Среди такой информации могут быть:

– секреты производства, ноу-хау;

– финансовая отчетность;

– сведения о сделках и коммерческих планах;

– инсайдерская информация, которую можно использовать для недобросовестного участия на рынках ценных бумаг,

– компрометирующие материалы на компании, их владельцев и менеджеров.

В марте 2016 года мир потряс скандал с панамской юридической фирмой Mossack Fonseca, утечка 11,5 млн документов из которой повлекла отставки глав государств и налоговые расследования в отношении политиков и знаменитостей.

Ущерб, причиненный данной утечкой, невозможно оценить. В то же время можно с уверенностью утверждать, что в результате подобной потери данных на репутации Mossack Fonseca поставлен крест.

Кстати, всего за месяц до атаки на Mossack Fonseca Федеральное Бюро Расследований США (ФБР) опубликовало официальное уведомление, предостерегающее, что некие лица подыскивают в хакерской среде исполнителей для взлома внутренних компьютерных сетей ряда крупных международных юрфирм.

Следует отметить, что американская пресса регулярно сообщает о кибератаках, жертвами которых становятся как юрфирмы среднего размера, так и гранды, например Cravath, Swaine & Moore. Следуя законам рынка, подобное развитие событий породило в США ажиотажный спрос на услуги страхования ответственности юристов на случай взлома их компьютеров и утечки данных. Следом возник спрос на профессиональное обеспечение компьютерной безопасности, которое позволяет снизить страховой тариф.

Российским адвокатам не грозят многомиллионные иски от клиентов с требованиями возместить убытки, связанные с некачественным оказанием юридической помощи, они пока чужды нашей правовой системе. Тем не менее, как указано выше, главные риски, исходящие от кибератак, – это утечка клиентских данных и, как следствие, потеря репутации, возможно, самого ценного актива в нашем деле.

Что же следует сделать юрфирме, которая раньше не занималась вопросами превенции киберугроз?

1 Аудит существующей компьютерной сети, порядка хранения и передачи данных.

2 Структурирование вероятных угроз. К основным факторам риска можно отнести: риски хакерской атаки со стороны процессуальных оппонентов и риски доступа к данным со стороны госструктур (чаще всего недобросовестных правоохранителей), которые впоследствии могут передавать информацию оппонентам.

3 Консультации со специалистами в области компьютерной безопасности. Кстати, классический айтишник, умеющий создать учетную запись почты на mail.ru, заменить картридж в принтере, переустановить операционную систему после сбоя, и специалист в области компьютерной безопасности – это, как правило, два абсолютно разных человека. Разумеется, чем выше уровень проектов, обслуживаемых фирмой, тем выше уровень риска атаки. И тем квалифицированнее должны быть специалисты. В настоящее время на рынке сформировалось несколько крупных игроков, способных на высоком уровне посодействовать в отстройке системы безопасности. Основные вопросы для обсуждения: организация компьютерной сети, порядок хранения и передачи данных, формирование эффективной системы защиты.

4 Работа с личным составом. Нет повести печальнее на свете, чем повесть о стикере с паролями, который услужливо наклеен на монитор. Второй распространенный сценарий – флешка с совершенно секретными данными, оставленная на рабочем месте в день, когда пришли с обыском. Именно поэтому наряду с техническими мероприятиями необходимо доступно разъяснять сотрудникам характер существующих угроз и основные способы противодействия им.

5 Фирмам, работающим с крупными клиентами, стоит взять в привычку регулярные (минимум 1–2 раза в год) проверки системы компьютерной безопасности. Небольшим фирмам и частнопрактикующим юристам следует не реже раза в месяц менять все значимые пароли (общеизвестно, что пароль должен быть сложным, 8 и более символов, содержать строчные и заглавные буквы и цифры). Именно слабые пароли до сих пор являются ахиллесовой пятой большинства сетей.

6 План действий в случае атаки – это абсолютная необходимость, равно как и план эвакуации при пожаре. В простой и понятной форме такой план должен разъяснять каждому сотруднику фирмы контактные данные лиц, ответственных за те или иные действия в случае атаки, способы связи с ними, порядок уведомления клиентов, правоохранителей об инциденте, порядок документирования происходящего.

Опыт нашего бюро показывает, что при системном подходе расходы на обеспечение кибербезопасности находятся в пределах 10% в структуре затрат, не связанных с оплатой труда. В то же время немалую часть работы берут на себя старшие партнеры, которые в «боевых условиях» получили навыки компьютерной безопасности при оказании юридической помощи по крупным клиентским проектам.

Учитывая возрастающую с каждым днем значимость киберугроз, профессиональным объединениям юристов (АЮР, ФПА, ОКЮ) следует в самое ближайшее время подготовить и опубликовать методические рекомендации для участников отрасли, в которых в доступной форме были бы разъяснены современные механизмы и алгоритмы защиты. Аналогичные инструкции уже выпущены ассоциациями юристов США, Великобритании, других стран и доступны в открытом доступе для изучения.

ГДЕ ТОНКО, ТАМ И РВЕТСЯ

ПОКА ГРОМ НЕ ГРЯНЕТ…

Павел МЕЙНГАРД,
руководитель практики «IT-инфраструктура»,
КСК групп,
г. Москва

Инциденты, связанные с утечкой информации, происходят достаточно часто, просто не всегда информация об этом попадает в СМИ. Причем подобные случаи нередки и в нашей стране.

Стоит отметить, что информация, которая хранится в юридических компаниях, представляет не меньшую ценность, чем сведения, содержащиеся в медицинских картах пациентов больниц. При этом, несмотря на то что для злоумышленников выгоднее покопаться в документах юридической компании, чем в картотеке поликлиники, российское законодательство регулирует лишь вопросы сохранности персональных данных (Закон № 152-ФЗ).

Опыт работы экспертов КСК групп в сфере информационной безопасности составляет порядка 20 лет, и при этом на память не приходит ни одной юридической компании, в которой бы вопросам защиты конфиденциальной информации уделялось бы должное внимание. Хотя, возможно, причина в том, что к нам обращаются уже после того, как возникли проблемы.

Заметьте, несмотря на законодательное преследование лиц, совершивших кражу или грабеж, сберкассы тем не менее продолжают усиленно охранять! Важная информация также нуждается в защите.

Не следует забывать, что в XXI веке охота за компьютерной информацией – очень прибыльный бизнес. Атаки с помощью вирусов и специальных закладок в спаме стали повседневной рутиной и уже давно никого не удивляют. Также развивается социальный инжиниринг, совершенствуется инструментарий, позволяющий выявлять уязвимые места в программном обеспечении компании или ее оборудовании. В наше время промышленный и компьютерный шпионаж – целая индустрия с миллиардными оборотами.

Итоги расследований обстоятельств утечек информации красноречиво свидетельствуют о том, что фундамент для возникновения проблем в будущем, как правило, был заложен в момент, когда руководители компании произнесли фразы: «Мы так уже не первый год работаем, и ранее ничего страшного не случалось», «Нам так удобнее, не хотим ничего менять» и т. п. То есть эти ситуации вполне можно было предвидеть. В нашей практике было множество примеров, когда клиент был предупрежден об опасности, но риски не показались ему значимыми, и важная информация в результате попала к злоумышленникам. Вот уж точно пока гром не грянет…

Обратите внимание, целью злоумышленников подчас является не конкретный клиент компании, а сама компания, так как инцидент с компрометацией всех или большинства ее клиентов является приговором для фирмы – держателя информации.

По нашему мнению, для обеспечения информационной безопасности юридической компании вполне можно взять за основу требования того же Закона № 152-ФЗ. Несмотря на то что этот акт активно критикуют, представляется абсолютно разумным ограничение доступа персонала к ценной информации таким образом, чтобы сотрудник мог знакомиться только с теми данными, которые нужны ему для выполнения своих обязанностей. К остальной информации должны иметь доступ минимальное количество работников, которые несут персональную ответственность в случае утечки. Также важно использовать лицензионный и постоянно обновляемый антивирус.

Кроме того, требования Закона № 152-ФЗ предусматривают ряд грамотных административных и технических мер по систематизации и планированию информационной безопасности. Если ответственно, а не формально подойти к выполнению этих требований, то результат будет соответствующим. Большую часть требований можно выполнить своими силами, тем более если речь идет о юридической компании. Но наиболее сложные моменты, например, такие как разработка модели угроз, имеет смысл доверить профессионалам.

Необходимо отметить, что без понимания проблемы и возможных рисков со стороны руководства компании никакие законы не помогут защитить данные. Но здравый смысл, трезвый расчет и информированность помогут избежать неприятностей и в отсутствие законодательных подсказок.

НЕЛЬЗЯ ЭКОНОМИТЬ НА БЕЗОПАСНОСТИ

Артём ПЛАТОНОВ,
ведущий юрисконсульт, департамент налоговой безопасности, международного планирования и развития, КСК групп,
г. Москва

В действующем законодательстве Российской Федерации существует определенный перечень нормативных актов, относящих те или иные сведения, в том числе налоговую, банковскую, адвокатскую, аудиторскую тайну, к категории информации ограниченного доступа.

Однако в первую очередь стоит обратить внимание на Федеральный закон «О коммерческой тайне», поскольку именно он, по мнению законодателей, призван должным образом обеспечивать конфиденциальность определенной информации, в том числе полученной от контрагентов.

Согласно положениям указанного Закона обладатель информации, составляющей коммерческую тайну, правомочен самостоятельно определять круг лиц, имеющих доступ к конфиденциальной информации, надлежащим образом регламентировать отношения по использованию информации, составляющей коммерческую тайну, с работниками и контрагентами.

Кроме того, обладатель информации, составляющей коммерческую тайну, должен обеспечить достаточные меры, исключающие несанкционированный доступ к соответствующей информации, имеющей конфиденциальный характер.

Закон «О коммерческой тайне» в большей степени регламентирует отношения внутри организации – обладателя информации, составляющей коммерческую тайну, тем самым делая упор на человеческий фактор, что, впрочем, весьма обоснованно, поскольку именно рядовые сотрудники, которые являются непосредственными исполнителями поставленных перед ними руководством задач, имеют прямой доступ к конфиденциальным сведениям.

В юридических фирмах вопрос обеспечения сохранности конфиденциальной информации клиента обязан быть особенно четко отстроен, в том числе путем предоставления доступа к соответствующей информации только проверенным, опытным и, что немаловажно, лояльным сотрудникам, так как цена просчета в этом вопросе фатальна. Именно поэтому важно при выборе консультантов отдавать предпочтение фирмам, безупречно зарекомендовавшим себя на рынке на протяжении не одного десятка лет.

Профессиональные консультанты всегда придерживаются деловой этики, которая не позволяет пренебрежительно относиться к коммерческим тайнам своих клиентов, чувствуя особую ответственность за сохранность полученных сведений, поскольку визитной карточкой юридической фирмы, на наш взгляд, является ее репутация.

Для целей обеспечения информационной безопасности юридической фирмы необходимо не только выстроить IT-безопасность, но и с определенной периодичностью проводить ее аудит.

Учитывая печальный опыт компании Mossack Fonseca, можно сделать однозначный вывод о чрезвычайной важности иметь защищенный IT-блок. Экономить на безопасности недопустимо!

В заключение хочется отметить, что нарушение требований Закона «О коммерческой тайне» влечет за собой не только дисциплинарную, гражданско-правовую и административную ответственность, но и уголовную в соответствии со ст. 183 УК РФ.

БЕЗ ЗЛОГО УМЫСЛА

Клаус ПФАЙФЕР,
директор по правовым решениям,
компания Thomson Reuters,
г. Москва

Кто владеет информацией, тот владеет миром. Одним из ключевых критериев при выборе юридических консультантов, помимо профессионального уровня подготовки, является умение обращаться с предоставленными данными, которые в 90% случаев являются для заказчика информацией конфиденциальной и/ или информацией, подпадающей под режим коммерческой тайны. Другими словами, тем самым мостиком, который позволяет выстраивать долгосрочные партнерские отношения между клиентами юридических фирм и консультантами.

Утеря такой информации в юридических фирмах может происходить по разным причинам, среди которых основными можно назвать технологический и человеческий факторы, причем из этих двух очень сложно выделить один приоритетный. Случаи утечки информации можно разделить как на умышленные, так и совершенные по неосторожности. Работая с человеческим и технологическим факторами и предотвращая случайные и умышленные утечки или минимизируя их последствия, мы выстраиваем комплексную линию защиты информации для юридической фирмы, затрагивающей как технологическую составляющую процесса, так и контроль влияния человеческого фактора (включая превентивные меры).

Если говорить про человеческий фактор в части умышленных преступлений, то юридической фирмой как держателем доверенной ей информации должны быть созданы такие условия, которые не позволят сотруднику даже помыслить о совершении противозаконных действий с оперируемыми данными. Развитие корпоративной культуры, в которой этике и морали придается ключевое значение, мотивация сотрудников и не в последнюю очередь установление так называемого Tone from the top, то есть стиля поведения, стандартов поведения и ведения бизнеса, задаваемого руководством, – все это позволяет создать условия, которые минимизируют риски распространения информации, вызванные наличием человеческого фактора.

Однако значительное количество случаев утечки информации происходит даже при отсутствии злого умысла просто потому, что сотрудники не обладают необходимыми знаниями относительно способов хранения конфиденциальной информации либо ненадлежащим образом относятся к выполнению требований, установленных работодателем, в указанной сфере. Поэтому тренинги по информационной безопасности и комплайенс, а также обучение в целом должно стать неотъемлемой частью профессионального развития любого сотрудника.

В области предотвращения преступлений, совершаемых по неосторожности, очень важно, чтобы сотрудники фирмы знали, что делать, чтобы не стать жертвой таких случайных утечек, и что делать, если информацию все-таки украли. Спросите своих сотрудников: знают ли они, что делать, если у них украли ноутбук? Как управлять своими паролями? Есть ли у них пароли на компьютере? Блокируют ли они экран каждый раз, когда уходят? Оставляют ли они ноутбук в офисе непристегнутым в случае отсутствия на рабочем месте? Пользуются ли личной почтой в служебных целях? Если ответ хотя бы на один из таких вопросов утвердительный, стоит, на наш взгляд, провести специальное обучение для сотрудников. Звучит банально, но зачастую именно это помогает защитить репутацию фирмы.

Таким образом, мы сможем значительно снизить риски, связанные со случайными нарушениями, приведшими к потере или утечке данных, и минимизировать риски, связанные с умышленным распространением информации.

Если говорить про технологическую сторону вопроса, то здесь важно отметить несколько ключевых моментов, на которые следовало бы обратить внимание. Во-первых, это, конечно, осознанный выбор программного продукта, используемого вашей фирмой. Это должен быть зарекомендовавший себя программный продукт, производитель которого имеет долгую историю и уделяет значительное внимание информационной безопасности.

Второй важный аспект технологической стороны вопроса – это регулярные и своевременные обновления систем. Любое ПО, каким бы оно хорошим и надежным ни было, требует регулярных обновлений. Кстати, по одной из версий нашумевшего дела Mossack Fonseca, утечку информации связывали именно с ПО, которое не было вовремя обновлено.

Еще очень важные моменты, которые, к сожалению, упускаются во многих компаниях, – это управление правами доступа, возможность отслеживать изменения в документах с четкой идентификацией того, кто эти изменения произвел, и прочие, возможно, выглядящие простыми, но в то же время очень действенные вещи.

Все эти меры, конечно, не гарантируют юридической фирме защиту от утечки информации, но помогут значительно снизить риски. В деле безопасности нет мелочей!

№ 35
СЕНТЯБРЬ 2016
ЭЖ ЮРИСТ

ЗАЩИТА ИНФОРМАЦИИ...

НУЖНЫ НАДЕЖНЫЕ СОТРУДНИКИ

Иван ХАПАЛИН,
адвокат, управляющий партнер,
Центр правовых отношений,
г. Москва

Закономерно, что защищенность информации в юридической фирме играет важную роль. Даже компании, занимающиеся научными разработками, могут понести меньший для себя ущерб после распространения информации, работа над которой велась годами.

История с офшорами показательна не столько с точки зрения утечки информации, сколько с точки зрения того, какую ценность и значимость зачастую представляет собой информация, скрытая за толстыми папками в сейфах юридических компаний. Первое и наиболее банальное требование – подписание соглашения о неразглашении всеми принимаемыми в компанию сотрудниками. Конечно, правило настолько элементарно, что напоминать о нем странно, тем более тем, кто сам занимается юридической деятельностью.

Тем не менее такой элементарной нормой весьма часто пренебрегают. Удивительно и в то же время закономерно: почти в 100% случаев утечка информации имеет под собой человеческий фактор. Можно сказать, что малым и средним компаниям по большому счету больше не о чем заботиться. Вряд ли кто-то будет искать особый доступ к данным компании напрямую или через сетевой доступ. Исключения могут составить лишь случаи с громкими делами, известные как минимум во всем регионе.

Базовую безопасность необходимо обеспечивать опять же там, где есть связь с человеческим фактором, по возможности не использовать телефонную связь для передачи сколько-нибудь значительных данных, касающихся клиентов. При необходимости использовать мессенджеры с криптошифрованием. Важно не позволять сотрудникам совмещать функции корпоративной и личной почты. Надо понимать, что чем больше формальных требований к безопасности будет введено в вашей компании, тем выше будет соблазн сотрудников нарушить правила в самой грубой форме. Прежде всего нужно внимательно относиться к тому, насколько подготовлены ваши сотрудники к сохранению секретов.

ДОВЕРИЕ – ГЛАВНОЕ

Дмитрий КАЗАКОВ,
адвокат, управляющий партнер, Адвокатское бюро «Казаков и Партнеры»,
г. Москва

В контексте событий, связанных с утечкой информации из панамской юридической компании Mossack Fonseca, следует понимать разницу между видами деятельности, которые данная компания обозначает публично, и тем, чем она занимается на самом деле. Кроме того, необходимо учитывать специфику юридических услуг, оказываемых этой компанией и внутрироссийскими юридическими фирмами.

Формально юридическая компания Mossack Fonseca просто помогает создавать юридические лица. Фактически же ею предоставляется комплекс услуг по очистке денег (сокрытие источника происхождения средств) и/или уменьшению налогообложения, исходя из принципа интернациональности. Соответственно скандал с обнародованием данных этой компании, именуемый «Панамагейтом», разворачивался вокруг фигур, воспользовавшихся услугами компании предположительно для достижения именно таких целей – очистки средств, выведенных из одних стран в другие, и уменьшения их налогообложения. Позиция руководства компании, комментирующего ситуацию, строится вокруг формальной стороны деятельности компании: создание юридических лиц не влечет для компании ответственности за их дальнейшее использование.

В нашем национальном законодательстве вопрос защиты информации такого рода не разрешен в связи с отсутствием соответствующих отношений. Российская практика обеспечивает возможность использования правоохранительных органов для доступа к любой информации внутри страны, кроме содержащей государственную тайну.

Поэтому наибольший интерес в России в плане инсайдерской деятельности представляют именно данные государственных органов, а не коммерческих организаций. Соответственно наиболее громкие случаи утечки информации касались распространения данных МВД, налоговых органов (2004 год, по некоторым данным, информация была украдена из базы Пенсионного фонда), а также Центробанка (2005 год). Из коммерческих структур знаковые случаи утечек зафиксированы только у операторов связи, причем практически у всех крупных (МТС, «БиЛайн» и «МегаФон»).

Структуры, аналогичные панамской юридической фирме, в России, безусловно, работают. Но, как правило, системы юридических лиц, в том числе с офшорными компаниями, для целей вывода средств и уменьшения налогообложения создаются не для оказания услуг неограниченному кругу клиентов, а под конкретные проекты, под конкретных заказчиков. Так, деятельность Центробанка по проверке деятельности коммерческих банков в основном состоит в выявлении структур, позволяющих выводить активы банков под видом невозвратных и необеспеченных кредитов.

В связи с этим обеспечение информационной безопасности для юридической фирмы в России не имеет принципиальных отличий от такого рода мероприятий для любого иного вида бизнеса. В самом общем виде этот вопрос можно обозначить как комплекс мероприятий по определению информационных полей, на которые распространяется требование о конфиденциальности, и, что самое проблематичное, круга лиц, допущенных к конфиденциальной информации. Все значительные случаи утечки информации в России отмечены действиями инсайдеров, что определяет фактор доверия при допуске к информации как наиболее важный в вопросе защиты информации.

ЧТО ГРОЗИТ ИНСАЙДЕРУ?

Елена ЧЕРНОКАЛЬЦЕВА,
генеральный директор, ООО «Корпоративная солидарность»,
г. Санкт-Петербург

Самые серьезные утечки информации происходят изнутри – так называемый инсайд. Юридические компании страдают от инсайдеров не меньше остальных, чего только стоят недавние громкие скандалы с публикацией «панамского досье», поэтому они более чем серьезно подходят к вопросам конфиденциальности.

Законодательство, карающее за неправомерный доступ и разглашение коммерческой тайны, достаточно суровое. Статья 183 УК РФ устанавливает санкции от штрафа 500 тыс. руб. до двух лет лишения свободы.

Однако просто ли покарать инсайдера, который слил оппонентам-конкурентам горячую информацию? Не всегда.

Допустим идеальные условия: инсайдер пойман с поличным. Какова вероятность, что он будет привлечен к уголовной ответственности?

С точки зрения закона коммерческая тайна – это не конкретная информация, а режим сохранения ее в тайне от других, то есть технические средства защиты, определенный порядок доступа к информации, определение, что конкретная информация является конфиденциальной, и т. д. Для этого в компании обязательно должны быть внутренние локальные акты, которые определяют режим коммерческой тайны, а конкретный инсайдер должен быть ознакомлен под роспись с тем, что информация, на которую он покусился, является конфиденциальной.

Поэтому все не так просто. Хотя в коммерческих компаниях (кроме юридических) уровень передачи конфиденциальной информации на сторону достаточно высок, скандалы с наказанием инсайдеров в уголовном порядке компании стараются не раздувать.

Работодателю проще уволить попавшегося информационного воришку или разобраться с ним за пределами правового поля, чем обращаться в правоохранительные органы. Раскрывать сотрудникам МВД систему защиты информации, внутренние документы, остальную информацию, которая может составлять коммерческую тайну, доказывать, что именно эта информация потенциально давала преимущества перед конкурентами, мало кто решится. Менее всего готовы к этому владельцы и руководители юридических компаний, которые хорошо знают, сколь неповоротлива и непредсказуема бывает правоохранительная система.

Мой опыт говорит о том, что способы защиты информации в юридических компаниях не сильно отличаются от тех же действий в других коммерческих структурах. Большое значение имеют профессиональная этика юристов и бережное отношение к самому главному капиталу юриста – его репутации.

ЧЕЛОВЕЧЕСКИЙ ФАКТОР

Алексей МОРОЗ,
управляющий партнер,
Адвокатское бюро «Эксиора»,
г. Москва

Общие положения о защите информации закреплены в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Кроме того, ряд специальных законов регулирует отношения, связанные с защитой отдельных видов информации: государственной тайны (Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»), коммерческой тайны (Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»), банковской тайны (Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности»), налоговой тайны (ст. 102 НК РФ), тайны совершения нотариальных действий (Основы законодательства РФ о нотариате, утв. ВС РФ 11.02.1993 № 4462-1), тайны усыновления (ст. 139 СК РФ), врачебной тайны (Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ»), персональных данных (Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных») и др.

Положения о защите адвокатской тайны, то есть любых сведений, связанных с оказанием адвокатом юридической помощи своему доверителю, закреплены в ст. 8 Федерального закона от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в РФ»).

За нарушение законодательства о защите информации установлена административная ответственность (глава 13 КоАП РФ) и уголовная ответственность (ст. 183, 185, 272–274, 283–284, 138, 155 УК РФ).

Таким образом, российское законодательство в сфере обеспечения информационной безопасности является достаточно полным и соответствует современным требованиям. Однако наличие эффективных правовых инструментов обеспечения информационной безопасности ни в коем случае не отменяет необходимости использования технических и организационных средств защиты.

Юридические фирмы, безусловно, должны уделять защите информации пристальное внимание, используя весь комплекс имеющихся в наличии средств. Защитить информацию, хранящуюся в юридической фирме в электронном виде, помогает использование различных программных и аппаратных средств защиты. Это ограничение физического доступа к источникам хранения информации извне, шифрование сетевых сообщений, использование брандмауэров в неизолированных сетях, применение современных систем контроля и управления доступом к данным и др.

Защитить клиентскую информацию, содержащуюся в бумажных документах, позволяет использование комплекса мер организационного характера. Например, полученные от клиентов оригиналы документов могут храниться не в офисе юридической фирмы, а в отдельном, специально оборудованном для этих целей помещении, доступ в которое имеет очень ограниченное число проверенных сотрудников.

Для проведения конфиденциальных переговоров в офисе юридической фирмы также может быть оборудовано специально защищенное помещение, исключающее возможность несанкционированной записи переговоров как внутри этого помещения, так и извне.

Наиболее уязвимый элемент в системе защиты информации – это ее пользователь, поэтому человеческий фактор в организации системы информационной безопасности необходимо учитывать в первую очередь.

Несанкционированный доступ к конфиденциальной информации может явиться как следствием банальной халатности сотрудников (например, использование личной электронной почты для пересылки служебной информации, подключение к компьютерной сети внешних накопителей информации без предварительной проверки на наличие вредоносных программ и т. п.), так и следствием умышленных действий (инсайда).

Злоумышленники, пытающиеся получить доступ к конфиденциальной информации, используют весь арсенал методов спецслужб, поэтому предотвращение таких атак является достаточно сложной, но вполне выполнимой задачей. Например, одним из способов получения несанкционированного доступа к конфиденциальной информации может являться внедрение сотрудника в трудовой коллектив, а одной из мер противодействия такому способу – ограничение количества размещаемых фирмой прямых вакансий и наем персонала с помощью кадровых агентств.

Конечно, тотальный контроль за работой с конфиденциальной информацией со стороны руководства юридической фирмой может вызывать некоторый дискомфорт у ее сотрудников, которые в подобных мерах могут видеть угрозу своему личному пространству. Поэтому важной задачей является формирование в корпоративной культуре общих ценностей с тем, чтобы каждый сотрудник искренне считал соблюдение конфиденциальности своим профессиональным долгом.