

УВОЛНЯЕМ СОТРУДНИКА за разглашение конфиденциальной информации



Анна Силинская

старший юрист Capital
Legal Services

Разглашение коммерческой тайны и персональных данных других работников – грубое нарушение дисциплины труда (подп. «в» п. 6 ч. 1 ст. 81 ТК РФ). И хотя уволить можно уже за однократный проступок такого рода, сделать это непросто.

Если работник будет оспаривать законность увольнения, суд обязательно проверит все обстоятельства. В пункте 43 Постановления Пленума ВС РФ от 17.03.2004 № 2 перечислены три условия, которые при этом необходимо соблюсти:

- разглашенные сведения относятся к коммерческой тайне или персональным данным другого работника;
- сведения стали известны работнику в связи с исполнением им трудовых обязанностей;
- работник обязывался не разглашать такие сведения.

Рассмотрим эти условия и сложности, с которыми сталкиваются работодатели.

1 В компании должен быть введен режим защиты конфиденциальной информации

Для этого нужно принять ряд локальных нормативных актов и ознакомить с ними работников:

Если работодатель обнаружил, что работник раскрыл конфиденциальную информацию, он может защищать свои интересы по-разному, даже инициировать уголовное преследование. Безусловно, дальнейшая работа такого субъекта в компании немыслима, а значит, начать нужно именно с прекращения трудовых отношений. Но уволить сотрудника за длинный язык не так-то просто – придется соблюсти несколько условий.

- положение о коммерческой тайне и положение о персональных данных (определяющие состав, порядок работы и уничтожения конфиденциальной информации);
- приказ об определении списка лиц, имеющих доступ к коммерческой тайне, персональным данным, либо приказ о предоставлении разового доступа к такой информации.

Работодателю также нужно внедрить и выполнять ряд организационных и технических мер, обеспечивающих фактическое соблюдение режима конфиденциальности:

- установить пропускной режим;
- присвоить индивидуальные логины и пароли для входа работников в рабочие компьютеры и базы данных;
- вести журнал учета доступа лиц к конфиденциальной информации;
- нанести гриф «коммерческая тайна» на документы, содержащие конфиденциальную информацию.

По последнему пункту судебная практика неоднозначна.

ПРИМЕР

Одни суды указывают, что если на документах нет грифа «коммерческая тайна» с указанием обладате-

ля этой информации и учета лиц, получивших к ней доступ, значит, в отношении этих документов режим коммерческой тайны нарушен не был (Апелляционное определение Санкт-Петербургского городского суда от 23.06.2015 по делу № 33-10630/2015).

Другие полагают, что отсутствие грифа «коммерческая тайна» на разглашенной работником информации не имеет значения, поскольку это не говорит о том, что в них нет информации, содержащей коммерческую тайну (Апелляционное определение Московского городского суда от 08.06.2015 по делу № 33-19433/2015).

Наш совет Нанесите на документы, имеющие для компании особую ценность, гриф «коммерческая тайна». Это минимизирует риск того, что суд признает увольнение работника незаконным из-за отсутствия в компании режима коммерческой тайны.

2 Разглашенные сведения должны быть доверены работнику непосредственно работодателем

Работа с конфиденциальной информацией должна входить в должностные обязанности сотрудника. Это указывается в трудовом договоре, должностной инструкции, приказах о распределении обязанностей или ином документе (Кассационное определение ВС Удмуртской Республики от 15.06.2011 по делу № 33-2048/11). Если такая информация стала известна работнику случайно или от третьих лиц, его нельзя уволить по данному основанию.

ПРИМЕР

Увольнение за разглашение коммерческой тайны признано незаконным, поскольку работник узнал

Выявление факта разглашения

Интересующее нас нарушение, как правило, совершается скрытно и не всегда обнаруживается работодателем. Так, если конфиденциальная информация была раскрыта устно и доказательств этого факта не осталось, то выявить его и привлечь работника к ответственности практически нереально. Но это не значит, что работодатель не может контролировать соблюдение режима конфиденциальности.

Чтобы отслеживать утечку конфиденциальной информации, необходимо контролировать электронные каналы связи, используемые работниками в рамках

информацию о размере заработной платы коллег от бывшего сотрудника компании (Определение ВС Республики Коми от 09.02.2012 по делу № 33-594/2012).

3 Работник обязался не разглашать конфиденциальные сведения

Работник должен в письменном виде принять обязательство не разглашать конфиденциальную информацию. При этом каких-либо определенных требований к виду соответствующего документа нет. Это может быть трудовой договор, локальный акт (с которым работник ознакомлен под подпись) или отдельное соглашение (Апелляционное определение Московского городского суда от 08.09.2014 по делу № 33-18661/2014).

ПРИМЕР

Суды признают увольнение незаконным, если работник не давал обязательства не разглашать коммерческую тайну или персональные данные других работников (Кассационное определение ВС Республики Татарстан от 29.07.2010 по делу № 8674/10). При этом работодатель может не заключать отдельное соглашение об обязательстве работника не разглашать конфиденциальную информацию, достаточно прописать его в трудовом договоре (Апелляционное определение Московского городского суда от 08.09.2014 по делу № 33-18661/2014).

Несоблюдение любого из рассмотренных условий служит самостоятельным основанием для признания увольнения работника за разглашение конфиденциальной информации незаконным.

служебной деятельности. Коллизия такого контроля заключается в столкновении интересов работодателя, защищающего конфиденциальные сведения компании, с конституционными правами работников на личную переписку и частную жизнь (ст. 23 Конституции РФ).

Так, с одной стороны, информация, находящаяся на рабочей почте работника, является исключительно средством осуществления его трудовых функций в интересах работодателя. С другой стороны, на рабочей почте хранится и личная переписка работ-

ников, просмотр которой потенциально может нарушить их конституционные права.

ПРИМЕР

Контроль за использованием рабочей почты, телефона, компьютера со стороны работодателя не нарушает конституционных прав работника на личную переписку и частную жизнь при условии своевременного предупреждения последнего о таком контроле (Постановление ЕСПЧ «Копланд против Соединенного Королевства» от 03.04.2007 по жалобе № 62617/00).

Позиция ЕСПЧ воспринята и российскими судами. Таким образом, чтобы законно проверять рабочую почту, телефон, компьютер сотрудника и использовать добытые таким образом доказательства в качестве основания для увольнения, необходимо, чтобы работник был предупрежден о возможности проведения таких контрольных мероприятий заблаговременно и под подпись.

Подчеркнем, что проверка работодателем личных средств связи работника является нарушением его конституционных прав на личную переписку и частную жизнь.

ПРИМЕР

Просмотр работодателем сообщений личной электронной почты со служебного компьютера ограничивает конституционное право на тайну переписки, тем самым противоречит Конституции РФ. Даже если в личной почте работника обнаружены следы передачи конфиденциальной информации третьим лицам, работодатель не может основываться на них при наложении дисциплинарного взыскания, поскольку он получил их с нарушением тайны переписки (Решение

Ворошиловского районного суда г. Волгограда от 25.07.2011 по делу № 2-2770/2011).

Дискуссионным остается вопрос о том, как квалифицировать передачу работником по электронной почте самому себе или своим родственникам сведений, составляющих коммерческую тайну, или персональных данных других работников, а также копирование такой информации на внешние носители. Судебная практика не отличается единообразием.

ПРИМЕР

В одних решениях суды говорят, что при передаче конфиденциальных сведений определяющим фактором выступает наличие доказательств распространения работником информации третьим лицам. Если они не представлены, то передача или копирование таких данных не является разглашением (Определение Московского городского суда от 16.11.2011 по делу № 33-33814).

Однако порой суды признают разглашением передачу сообщений, содержащих конфиденциальные сведения, самому себе на личную почту. Ведь при этом задействованы почтовые агенты (Яндекс, Мэйл, Рамблер), которые имеют доступ ко всем электронным сообщениям (Апелляционное определение Московского городского суда от 08.09.2014 по делу № 33-18661/2014).

Кроме того, копирование конфиденциальной информации на внешние носители даже при отсутствии доказательств ее распространения при нарушении режима коммерческой тайны, защиты персональных данных признается судами разглашением (Апелляционное определение Московского городского суда от 04.08.2015 по делу № 33-24617/15).

Наш совет

Чтобы законно проверять рабочую почту, телефоны, компьютеры работников и использовать полученные доказательства в качестве основания законного увольнения, необходимо:

- в локальных актах компании запретить работнику:
 - использовать рабочие средства для ведения личной переписки с другими сотрудниками или третьими лицами;
 - передавать конфиденциальную информацию третьим лицам, самому себе на личную почту или своим родственникам, а также копировать ее на внешние носители;
- предусмотреть полномочие работодателя осуществлять мониторинг рабочей почты, телефона, компьютера работника с целью контроля над соблюдением политик компании и уведомить работника о таком полномочии под подпись;
- создать в компании службу безопасности для осуществления контроля (или делегировать эти функции IT-отделу);
- регулярно контролировать рабочие средства связи с учетом максимального срока привлечения к дисциплинарной ответственности (6 месяцев с момента совершения проступка).

Фиксация нарушения и увольнение

Итак, работодатель обнаружил факт разглашения конфиденциальной информации и установил наличие оснований для увольнения. Но этого недостаточно для того, чтобы увольнение было признано законным. Важно правильно зафиксировать нарушение и соблюсти все процедуры и формальности, предусмотренные ТК РФ.

1 Составить докладную записку на имя непосредственного руководителя работника или руководства компании об обнаружении факта разглашения конфиденциальной информации.

2 На основании докладной записки издать приказ о создании комиссии, которая проводит внутреннее служебное расследование: собирает доказательства, исследует обстоятельства дела, анализирует и дает оценку действиям работника.

3 В процессе служебного расследования необходимо запросить у работника объяснения его неправомерного поведения. Они должны быть приняты и учтены комиссией при выяснении обстоятельств дела и последующем вынесении окончательного решения.

4 Если работник отказывается от дачи объяснений или не предоставляет их в течение двух рабочих дней с момента запроса, следует составить соответствующий акт. Данное обстоятельство не мешает комиссии вынести решение по итогам служебного расследования и привлечь работника к дисциплинарной ответственности.

5 По итогам выяснения всех обстоятельств дела комиссия составляет акт о результатах служебного расследования, в котором дает оценку действиям работника и делает выводы о необходимости привлечения его к дисциплинарной ответственности.

6 Если с учетом этого акта работодатель принимает решение о привлечении работника к дисциплинарной ответственности, в частности об увольнении, издается приказ. С ним сотрудник должен быть ознакомлен под подпись в течение трех дней после издания. Привлекая работника к дисциплинарной ответственности, соблюдайте сроки, установленные ТК РФ (по общему правилу – не позднее 1 месяца со дня обнаружения проступка и 6 месяцев со дня его совершения).

7 Если увольнение носит конфликтный характер и существует риск его оспаривания (а при записи в трудовой книжке об увольнении за разглашение конфиденциальной информации это весьма вероятно), желательно дополнительно зафиксировать нарушение с помощью нотариального протокола осмотра доказательств. Для этого необходимо вызвать сотрудника, разгласившего конфиденциальные сведения. Процедура протоколирования может проводиться как через удаленный доступ в кабинете у нотариуса, так и в самом офисе работодателя, если последний не желает предоставлять третьим лицам доступ к корпоративным компьютерам. Зафиксированное нотариусом доказательство будет иметь в суде больший вес, чем доказательство, распечатанное самим работодателем (например, электронная переписка).

При следовании приведенному алгоритму процедура привлечения к дисциплинарной ответственности будет соблюдена и риск признания увольнения незаконным по формальным основаниям станет минимальным.

Все это позволит компании не только привлечь нарушителя к ответственности за разглашение конфиденциальной информации, но и предотвратить такое разглашение. К сожалению, многие принимают подобные меры лишь постфактум, после возникновения проблемной ситуации, когда исправить что-либо уже сложно. Поэтому правильнее и эффективнее задуматься о защите информации заблаговременно.

Ищите нас на Facebook



корпоративный юрист

