Правовые аспекты контроля электронной почты

Электронная почта сегодня – это дешевый и удобный способ связи для получения информации извне, а также распространения информации между сотрудниками компании. Она позволяет оперативно управлять бизнес-процессами в организации, но вместе с тем является одним из наименее защищенных ресурсов корпоративной информационной системы.

> **Городничий.** *Послушайте, Иван Кузьмич, нельзя ли вам, для общей нашей пользы, всякое письмо, которое прибывает к вам в почтовую контору, входящее и исходящее, знаете, этак немножко распечатать и прочитать: не содержится ли в нем какого-нибудь донесения или просто переписки. Если же нет, то можно опять запечатать; впрочем, можно даже и так отдать письмо, распечатанное.*
>
> **Почтмейстер.** *Знаю, знаю... Этому не учите, это я делаю не то чтоб из предосторожности, а больше из любопытства: смерть люблю узнать, что есть нового на свете. Я вам скажу, что это преинтересное чтение. Иное письмо с наслажденьем прочтешь – так описываются разные пассажи... а назидательность какая... лучше, чем в "Московских ведомостях"!*
>
> ***Н. В. Гоголь. "Ревизор"***

Отсутствие контроля со стороны руководства или сотрудников службы безопасности за использованием электронной почты сотрудниками компании порождает ряд серьезных проблем: "утечка" конфиденциальной информации, распространение по локальной сети организации компьютерных вирусов и спама, использование сотрудниками корпоративной почты в личных целях. Отметим, что последнее приводит к потерям рабочего времени сотрудников, перегрузке каналов передачи информации и, как следствие, к неоправданному росту стоимости их содержания. При решении этих проблем необходимо использовать комплекс организационно-технических мер контроля корпоративной электронной почты.

Необходимость внедрения именно комплекса мер обусловлена тем, что одни только организационные меры неэффективны. Недостаточно создать политику использования корпоративной электронной почты, издать приказ или распоряжение, ознакомив с положениями этих документов сотрудников под роспись, необходимо еще иметь возможность контролировать выполнение этих директив техническими средствами, которые включают в себя контроль содержимого писем и ведения архива переписки по электронной почте.

Но в этом случае руководство компании сталкивается с иным риском – юридической ответственностью в части законности проверки почтового трафика и правом сотрудников на тайну личной переписки.

Разберем проблему противостояния работников и работодателей в этом вопросе подробно.

Каждый сотрудник имеет право

Согласно Конституции РФ (ст. 23), "каждый гражданин имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения".

Именно на эту статью чаще всего ссылаются сотрудники, если возникает вопрос о правомерности контроля со стороны работодателя переписки, ведущейся по корпоративной электронной почте, телефонных переговоров сотрудников, посещения ими тех или иных Интернет-сайтов. То есть законодательство РФ не дает работодателю права контролировать переписку сотрудников и не предусматривает возможности нарушать ее конфиденциальность.

Однако абонентом телефонной сети, оплачивающим переговоры, является организация — юридическое лицо, а вовсе не ее сотрудники. То же относится и к вопросам использования электронного почтового ящика. Тем не менее, многие сотрудники склонны рассматривать эти ресурсы, предоставленные им организацией в качестве инструмента для решения служебных задач, как элемент своей личной, частной жизни.

Каждый работодатель имеет право

Работодатель правомерно считает, что корпоративная электронная почта принадлежит компании. Соответственно, электронная почта должна использоваться сотрудниками только для выполнения ими служебных обязанностей и не предназначена для ведения личной переписки. Работодатель оплачивает почтовый трафик, используемый сотрудниками в личных целях, и рабочее время сотрудников, потраченное на личное общение. Очевидно, что в случае даже случайной "утечки" конфиденциальной информации по вине сотрудников, убытки понесет также работодатель, и желание владельца компании контролировать принадлежащий ей ресурс является вполне обоснованным.

Федеральный закон Российской Федерации дает работодателю право контролировать каналы возможной "утечки" конфиденциальной информации, в том числе и электронную почту сотрудников. В частности, ст. 10 ч. 4 Федерального закона Российской Федерации от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" гласит: "Обладатель информации, составляющей коммерческую тайну, вправе применять при необ-

ходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству Российской Федерации, меры".

Приведем еще ряд законов, которые работодатель может использовать в случае необходимости отстаивания своих прав:

- Закон РФ от 21.07.03 № 5485-1 "О государственной тайне".
- ФЗ от 27.07.06 № 149-ФЗ "Об информации, информационных технологиях и защите информации".
- ФЗ от 27.07.06 № 152-ФЗ "О персональных данных".

Однако, несмотря на достаточно большое количество законодательных актов, защищающих права владельцев компаний, руководителям организаций, внедряющим технические средства контроля каналов связи или передачи данных (в том числе и электронной почты), все же хочется знать, как в подобной ситуации остаться в рамках закона?

Организация контроля корпоративной электронной почты

Тайна переписки распространяется на лиц, участвующих в процессе переписки только при оплате этих средств и услуг оператора связи самостоятельно.

Служебная переписка организуется в производственных целях в рабочее время при помощи технических средств, принадлежащих организации. Если сотрудник организации включает в этот процесс личные мотивы и цели, то подобные действия можно рассматривать как удовлетворение личных потребностей за счет организации, что, соответственно, подпадает под действие УК РФ или КоАП РФ со всеми вытекающими для данного лица последствиями. То есть вся переписка, осуществляемая сотрудниками организации в рабочее время при помощи технических средств, принадлежащих данной организации, и по оплаченным ею каналам связи или передачи данных, является служебной, даже если таковая ведется в нерабочее время.

Для того чтобы все вышесказанное имело под собой правовую основу, руководителю организации необходимо выполнить ряд обязательных процедур:

1. Указать в уставе организации, кто является собственником всех материальных, технических и интеллектуальных (информационных) ресурсов, в том числе и содержимого служебной переписки, которая осуществляется сотрудниками организации в служебное время и при помощи технических средств, принадлежащих организации.

2. Создать в организации структурное подразделение информационной безопасности, на сотрудников которого возложить функции контроля соблюдения режима информационной безопасности. Основной задачей подразделения будет являться контроль технических средств обработки информации (ее приема, передачи и хранения), а также контроль служебных документов организации, к каковым относится и служебная переписка.

3. Издать "Положение о работе подразделения структурной безопасности". В документе должны быть четко описаны все процедуры контроля исполнения данного Положения: периодичность и средства его проведения, ответственные лица, форма отчетности.

4. Установить в организации режим коммерческой тайны (согласно ст. 10 ч. 1 закона "О коммерческой тайне"). Руководитель должен издать приказ, определяющий права доступа сотрудников к информации, носящей конфиденциальный характер. Служба безопасности или уполномоченные лица обязаны контролировать соблюдение сотрудниками требований к работе с подобной информацией в целях исключения ее "утечки". Отметим, что государство ограничивает права работника в данном вопросе и в том случае, если компания принадлежит частному лицу. Пример такого документа можно найти в справочно-правовой системе ГАРАНТ, набрав в графе "Поиск" следующую фразу: "Положение о конфиденциальной информации (коммерческой тайне) открытого акционерного общества".

5. При заключении с сотрудником трудового соглашения в контракт необходимо включить пункт, гласящий, что работодатель оставляет за собой право контроля деятельности сотрудника на рабочем месте в служебное время, в том числе проверку содержимого служебной переписки, каким бы способом она ни велась – на бумажных носителях, при помощи электронной почты или иным, возможно даже экзотическим способом. Письменная служебная переписка подшивается в папки и хранится много лет, а следовательно, всегда доступна для контроля. На сегодняшний день подобная организация делопроизводства возможна и применительно к электронной почте компании. Кроме того, работодатель имеет возможность включить в трудовой контракт пункт о запрете использования применяемых им средств передачи данных или иных технических средств, принадлежащих организации, в личных целях.

Подведем некоторые итоги. Для того чтобы у руководителей компании не возникло проблем с законом в вопросах организации информационной безопасности компании, юристы рекомендуют предпринять следующие меры:

- Создать перечень сведений, которые составляют коммерческую тайну предприятия и не подлежат разглашению, и ознакомить с данным документом всех сотрудников организации.
- Включить в трудовой договор сотрудника пункт, запрещающий использование предоставляемых ему рабочих ресурсов в личных целях.
- Ознакомить сотрудников предприятия с процедурами обжалования действий контролирующих подразделений компании.

В свою очередь, сотрудникам организации для того, чтобы у них не возникло конфликтов с работодателем, юристы советуют соблюдать трудовую дисциплину и помнить, что личная переписка защищена законом лишь в том случае, если она ведется в свободное от работы время, на личном оборудовании и оплачивается ими самостоятельно.

Александр Синельников, эксперт центра информационной безопасности, компания "Инфосистемы Джет"