DLP и закон в вопросах и ответах

Говорят [1], что DLP (система защиты от утечек конфиденциальной информации) противоречит каким-то правам человека. Это так?

Использование DLP-системы в некоторых режимах действительно может нарушать права человека. А именно, право на тайну связи и право на тайну частной жизни.

Что такое тайна связи?

Тайна связи – это часть 2 статьи 23 Конституции РФ [2]. Она гласит: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения» Необходимо пояснить, что имеются в виду только сообщения, направленные человеком другому человеку по каналу, который в принципе предусматривает закрытость, непубличность. То есть, например, это право не касается обычного веб-трафика, поскольку обмен сообщениями происходит между человеком и не-человеком (публичным ресурсом).

Нарушает ли закон DLP-система?

Закон регулирует отношения между людьми. Поэтому нарушить закон может только человек. Любая система сама по себе нарушать закон в принципе не может. А вот использование той или иной системы определённым способом может являться правонарушением. Касательно DLP-систем, противозаконным является такое их использование, которое нарушает право на тайну связи, то есть предусматривает **ознакомление** с сообщением кого-либо кроме отправителя, получателя и уполномоченных ими лиц или **разглашение** сообщения. Если разглашения нет, ознакомления постороннего человека с сообщением нет или ознакомление санкционировано отправителем (получателем), то закон не нарушен.

Распространяется ли тайна связи на служебные каналы?

Да, распространяется. В статье 23 Конституции предусмотренное единственное ограничение права на тайну связи – по решению суда. Других ограничений, в частности, для служебных каналов, не предусмотрено [3].

Но предприятие владеет служебными средствами связи и оплачивает услуги связи. Значит, оно и распоряжается сообщениями. Ведь владелец ресурса вправе устанавливать любые правила использования этого ресурса. Разве не так?

Не так. Право собственности – не абсолютно. Владелец информационного ресурса (и любого другого имущества) вправе устанавливать правила его использования лишь в рамках, установленных законом. Кроме того, даже осуществляя свои законные права, владелец не может нарушать прав других лиц (это называется злоупотребление правом). В данном случае право собственности на средства связи не влечёт за собой права нарушать конфиденциальность личных сообщений, которая гарантирована Конституцией.

Работники ведь были официально предупреждены, что все их сообщения могут просматриваться. Это ведь снимает проблему?

Нет, не снимает. Перлюстрация чужих сообщений незаконна. Предварительное уведомление не превращает незаконное деяние в законное.

Предприятие обладает коммерческой тайной. И имеет право эту тайну защищать. Контроль каналов связи – всего лишь средство для сохранения коммерческой тайны. Правильно?

Не правильно. Обладание коммерческой тайной даёт её обладателю ряд прав, перечисленных в статье 7 закона «О коммерческой тайне». Там всего 7 прав, и список этот является закрытым, то есть никаких «и т.д.», «и др.». Среди перечисленных прав обладателя коммерческой тайны отсутствует право контролировать каналы связи. Впрочем, даже если б оно там было, то не действовало бы. Конституция имеет приоритет над федеральными законами. Противоречащие Конституции положения законов не действуют.

Работник, который использует служебную связь в личных целях, нарушает условия трудового договора. Разве это не даёт право работодателю контролировать канал связи?

Не даёт. Никакое нарушение не даёт основания в ответ ущемлять права нарушителя. Тем более, что использование служебных средств связи в личных целях – это всего лишь дисциплинарное нарушение. За него нарушитель может получить выговор, в предельном случае может быть уволен. А нарушение права на тайну связи – это уголовное преступление, предусмотренное статьёй 138 УК. За это офицер безопасности, просматривающий чужие сообщения, подлежит уголовной ответственности. Нравится вам такой «размен»?

Служебную связь не положено использовать в личных целях. Следовательно, офицер безопасности, просматривающий сообщения, не ожидает увидеть среди них личное. То есть, у него нет умысла. Значит, нет и состава преступления, верно?

Не верно. Использование казённых средств связи в личных целях носит в России повсеместный характер. На многих предприятиях это официально разрешено, иногда – разрешено с оговорками. А там, где официально запрещено, этот запрет не соблюдается. Поэтому надуманная ссылка на незнание реалий офицером безопасности, скорее всего, не пройдёт.

Отправитель и получатель ведь вправе ознакомить со своими сообщениями кого он пожелает – это не нарушает права на тайну связи. А каждый работник дал письменное согласие на ознакомление со всеми его сообщениями. Это устраняет проблему?

Возможно. На этот счёт у юристов имеется два мнения. Одни считают, что письменное согласие работника на ознакомление службы безопасности со всеми отправляемыми и получаемыми им сообщениями действительно является разрешением на ознакомление и снимает проблему. Другие юристы полагают, что разрешение на ознакомление с отдельным конкретным сообщением – это одно, а согласие на ознакомление с неопределённым множеством будущих, ещё пока не существующих сообщений – это уже не разрешение, а отказ от права на тайну связи. А любой отказ от права – недействителен

(ст. 17 Конституции). Таким образом, указанное письменное согласие работника не снимает проблему полностью, хотя и существенно снижает соответствующий риск.

А если в ходе работы DLP-системы человек с сообщениями не ознакамливается? Если весь анализ происходит автоматически, и подозрительные сообщения просто не пересылаются?

Как уже говорилось, нарушением права на тайну связи признаётся ознакомление постороннего лица с сообщением или его разглашение. Любой программный анализ сообщения – не нарушение. Блокирование или уничтожение сообщения – также не нарушение (во всяком случае, не нарушение права на тайну связи). Архивирование и хранение сообщения без ознакомления с ним – не нарушение.

А разве блокирование или уничтожение чужой информации законно?

Бывает и незаконно. Например, преступлением является создание и использование вредоносных программ (ст. 273 УК). Блокирование или уничтожение чужой информации как раз и является характеристикой вредоносной программы.

Что такое вредоносная программа?

Её определение содержится в статье 273 Уголовного кодекса РФ. Вредоносной признаётся программа, «заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». Это определение не идеально. Нуждаются в толковании термины «заведомо», «несанкционированный», «информация». Принципиальное значение имеет толкование «санкции» – кто именно вправе давать санкцию на перечисленные действия с информацией или с информационной системой? Подробно мнение автора изложено в отдельной статье [4], а вкратце можно сказать так: санкцию на уничтожение, блокирование, модификацию либо копирование информации вправе давать обладатель [5] этой информации, а санкцию на нарушение работы ЭВМ, системы ЭВМ или их сети – оператор информационной системы [6].

Кто уполномочен решать, какая программа вредоносная, а какая нет?

Это решается судом на основании заключения эксперта. Фактически вредоносность устанавливает эксперт.

Может ли DLP-система быть признана вредоносной программой?

В принципе, может. Но для этого необходимо одновременное выполнение нескольких условий. Программа должна предназначаться для несанкционированных действий над информацией, эти действия должны производиться без разрешения (явного или неявного) обладателя информации. Заметим, что здесь речь идёт об информации, а не о сообщениях. Отправитель или получатель сообщения – это далеко не то же самое, что обладатель информации, содержащейся в сообщении. Хостовая часть [7] DLP-системы, в принципе, может перейти грань дозволенного, если она будет устанавливаться на персональный компьютер без санкции обладателя информации, содержащейся на этом компьютере – наподобие троянской программы. Автору неизвестны DLP-системы с подобными характеристиками, но они, в принципе, возможны.

Какие ещё юридические риски связаны с DLP-системами?

В части 3 статьи 138 УК предусмотрена ответственность за изготовление или сбыт «специальных технических средств, предназначенных для негласного получения информации». Некоторые программы можно отнести к таким средствам. Но практики по данной статье почти нет.

Является ли DLP-система таким средством?

В общем случае не является. Отсутствует принцип «негласности» получения информации. Впрочем, не исключено, что кто-то создаст DLP-систему, основанную на принципе скрытности её действия. Вот в этом случае можно будет говорить об ответственности по ч.3 ст.138 УК. Но пока невозможно уверенно судить о перспективах признания какой-либо DLP-системы «предназначенной для негласного получения информации». Тем более, что производство и сбыт таких средств не запрещено совершенно, как вредоносных программ, а требует особого разрешения.

Выходит, что DLP всё время балансирует на грани закона?

Можно так сказать. Создание, внедрение и использование DLP-систем действительно несёт риски, связанные с нарушением закона разработчиком или пользователем. Избежать этих рисков не так просто. При проектировании и при внедрении обязательно следует привлекать юриста, квалифицированного в области ИТ либо айтишника, квалифицированного в области информационного права.

Николай Николаевич Федотов, главный аналитик «InfoWatch»

---

[1] Формулировки вопросов намеренно даны нестрогие, просторечные – в таком виде, в каком их обычно задают автору на лекциях, учебных курсах. Ответы же приводятся по возможности в строгой юридической форме.

[2] **http://www.gov.ru/main/konst/konst12.html**

[3] Подробности можно прочитать в статье «Тайна связи против технических средств защиты информации в Интернете» http://forensics.ru/zi-ts.html

[4] «Расширительное толкование терминов “вредоносная программа” и “неправомерный доступ”» http://forensics.ru/ras_tolkovanie.html

[5] Обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (ст.2 закона «Об информации…»)

[6] Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (ст.2 закона «Об информации…»)

[7] Компонент DLP-системы, который контролирует каналы, имеющиеся на рабочей станции (CD-привод, разъёмы USB и др.), следит за локальными файловыми операциями, а также препятствует попыткам обхода DLP.