УДК 004.056.5:34

**Журилова Е. Е., Шабуров А. С.**

# О НОРМАТИВНО-ПРАВОВЫХ АСПЕКТАХ ВНЕДРЕНИЯ DLP - СИСТЕМ

*В данной статье рассмотрена проблема соответствия внедрения программно-технических средств защиты информации требованиям законодательства Российской Федерации и морально – этическим нормам. Приведена схема, иллюстрирующая противоречие между применением DLP-систем и необходимостью защиты персональных данных в корпоративных системах предприятий и организаций. Предложены пути разрешения подобных противоречий.*

***Ключевые слова:*** *DLP система, соответствие, нормативно-правовой акт, мониторинг, утечка информации, конфиденциальность, этическая сторона.*

**Zhurilova E. E., Shaburov A. S.**

# ABOUT THE REGULATORY AND LEGAL ASPECTS OF DLP- SYSTEMS IMPLEMENTATION

*The article deals with problem of matching system of data leak prevention with legislation of Russia Federation and moral and ethical standards. It presents a diagram, shows the contradiction between the using DLP-system and the need to protect personal data in enterprise system in companies and organizations. It proposed the ways of resolving such conflicts.*

***Keywords:*** *DLP system, matching, legal act, surveillance, data leak, confidentiality, ethical aspect.*

В настоящее время организация защиты конфиденциальной информации играет существенную роль в обеспечении конкурентоспособности предприятий и организаций различных форм собственности. В тоже время, решение задач по защите различных видов конфиденциальной информации, отнесенной, в том числе, к коммерческой тайне, персональным данным может привести к возникновению противоречий с правовой точки зрения.

Данное противоречие заключается в необходимости сохранения в конфиденциальности информационных ресурсов, за счет использования современных способов и средств защиты информации. В то же время, использование подобных средств может быть связано с ограничениями прав субъектов персональных данных, участвующих в процессе информационного обмена.

На рис. 1 представлена схема, иллюстрирующая возникновение возможных противо-

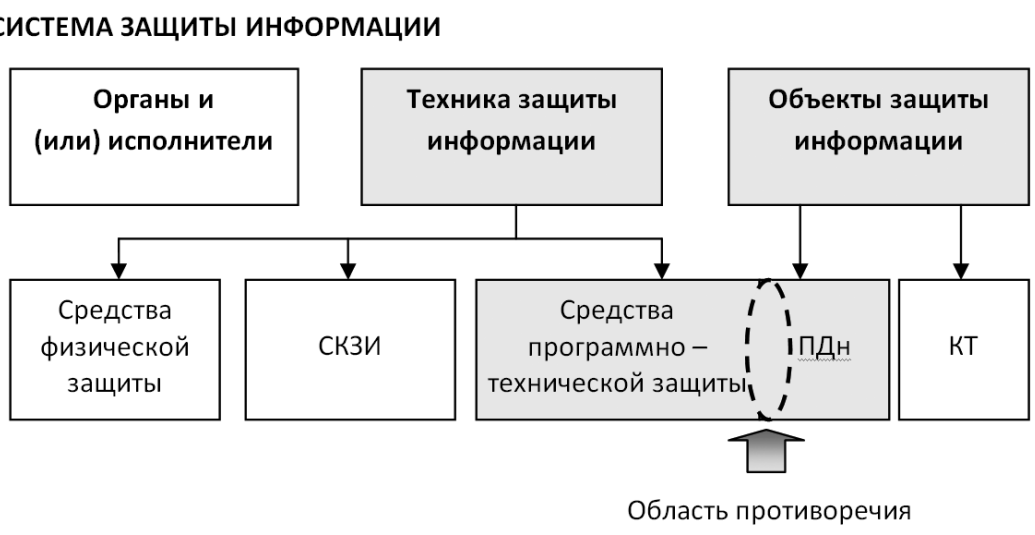


Рис. 1. Область возможного противоречия в системе защиты информации

речий между необходимостью применения программно-технических средств защиты информации и требований по осуществлению контрольных мероприятий на основе подобных средств. В данном случае процедуры контрольных мероприятий могут осуществляться с использованием персональных данных работника, подвергающегося проверке.

На сегодняшний день разработан комплекс нормативно - правовых документов, определяющих как категории и виды конфиденциальной информации, требования по обеспечения информационной безопасности подобных информационных ресурсов, так и перечень рекомендуемых для использования способов и средств защиты информации.

В соответствии с требованиями Федерального закона «О персональных данных» № 152 – ФЗ операторы обязаны обеспечивать конфиденциальность переданных им персональных данных при хранении и обработке этих данных [1]. Закон «О коммерческой тайне» №98 – ФЗ требует охранять данные, в отношении которых введен режим коммерческой тайны [2]. Закон «О Государственной тайне» №5485-1 определяет способы и меры, которые следует применять при работе и с государственной тайной, как на территории Российской Федерации, так и за рубежом [3]. Так же существует ряд стандартов и рекомендаций Банка России, определяющих работу с персональными данными в банковской системе.

Для выполнения требований информационной безопасности перечисленных выше информационных ресурсов разработано большое разнообразие технических и программных средств защиты информации, которые могут работать как в составе одной сложной системы, так и автономно.

Одной из разновидностей программных средств защиты информации являются DLP-системы (Data Leak Prevention) системы предотвращения утечки данных. Такие системы позволяют контролировать трафик рабочих станций: почтовый, веб-трафик, трафик программ обмена мгновенными сообщениям, документы, отправленные на печать, документы, переданные на переносные устройства, а также делать снимки рабочего стола, прослушивать микрофоны. Функциональные возможности таких систем достаточно разнообразны, что позволяет контролировать весь объем передаваемого трафика, обеспечивая тем самым более полную защиту информации от утечек.

При внедрении DLP-системы в корпоративную информационную систему предприятия возникает ряд актуальных вопросов соответствия выполняемых функций выбранной DLP-системы требованиям законодательства по соблюдению прав человека на личную и семейную тайну, а также возможности использования подобной системы с точки зрения морально - этических норм.

Современные DLP-системы в той или иной форме предоставляют администратору возможность настройки различных политик

безопасности, позволяют контролировать все данные, передаваемые пользователями с их учетных записей, протоколировать события, составлять статистику использования информационных ресурсов. Так же существует возможность контроля портов рабочих станций и сетевых принтеров. Перечисленные возможности облегчают контроль над информацией и обнаружение утечек информации, тем самым обеспечивают выполнение требования по безопасности информации, определенной законодательством Российской Федерации для информации ограниченного доступа.

В то же время, анализ соответствия применения DLP-систем на соблюдение норм права, оговоренных в части 1 статьи 63 ФЗ «О связи», возникают проблемы с неоднозначностью трактовки данной статьи. В соответствии с данной статьей «на территории Российской Федерации гарантируется тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных и иных сообщений, передаваемых по сетям электросвязи и сетям почтовой связи» [4]. Данная статья, так же, как и статья 23 Конституции Российской Федерации, может препятствовать использованию программно-технических средств защиты для предотвращения утечки информации, поскольку мониторинг почтового трафика может нарушить тайну переписки сотрудников.

Очевидно, что данный закон регулирует отношения между операторами связи, предоставляющими платные услуги связи, и их клиентами, а отношения между организацией и работником в большинстве случаев к таковым не относятся [5]. Следовательно, в данном случае, вышеуказанный закон не будет являться препятствием при внедрении DLP-системы.

Часть 2, статьи 23 Конституции РФ гласит: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения [6]». Наличие статьи 23 Конституции Российской Федерации так же ставит вопрос законности внедрения и использования DLP-систем, поскольку мониторинг трафика пользователей включает мониторинг их почтовых сообщений в корпоративных сетях, что является незаконным на основании данной статьи Конституции.

Существует несколько возможных вариантов решения для данной проблемы.

Самым очевидным и наиболее часто используемым способом разрешения противоречия является оповещение сотрудников организации о внедрении DLP-системы и взятие у них письменного согласия на мониторинг трафика их рабочих станций организацией. Однако, подобный вариант разрешения противоречивой ситуации может являться противоправным. Поскольку сотрудники дают организации согласие на просмотр не только уже существующих сообщений, но и их будущего неопределенного количества, то с формальной точки зрения такое согласие может рассматриваться как отказ от права на тайну переписки, который является недействительным согласно части 2, статьи 17 Конституции РФ. Указанная статья гласит: «Основные права и свободы человека неотчуждаемы и принадлежат каждому от рождения» [6]. Поскольку право на тайну переписки является основным правом человека, и, следовательно, оно неотчуждаемо, то нельзя взять у сотрудников согласие на просмотр всех их сообщений в корпоративной сети.

DLP- система предоставляет возможность настройки различных политик безопасности. Поэтому, другим возможным решением проблемы нарушения права на тайну переписки, при внедрении системы, может являться настройка корректной политики ее работы.

Корректной политикой, в данной ситуации, будет являться такая политика, которая позволит DLP-системе самостоятельно разделять сообщения на личные и относящиеся к корпоративной переписке. Для этого система может использовать разнообразные метки и ярлыки, не прибегая к помощи оператора в процессе сортировки. Поскольку в данном случае распределение и сортировку сообщений будет производить программа, не являющаяся субъектом права, предоставляя оператору системы для мониторинга только корпоративную почту, то такой способ не нарушает ни требования законодательных актов, ни право человека на тайну переписки.

В большинстве систем можно настроить два варианта политики: либо личные сообщения в любом случае будут скрыты от оператора, независимо от обнаружения в них конфиденциальной информации, либо, в случае обнаружения конфиденциальной информации, оператор будет просматривать данное

сообщение. Оба варианта являются несовершенными. В первом случае будет нарушена непрерывность защиты информации, и данные будут уходить через личную переписку, без всякого контроля, что приведет к разглашению конфиденциальной информации. Во втором случае, опять же возникает нарушение конституционного права человека на тайну переписки. При этом не следует исключать определенный процент ошибок, связанный с критериями отбора личных и корпоративных сообщений. Таким образом, в настоящее время не представляется возможным составить абсолютно корректные правила разделения подобных групп [7].

Третьим решением данной проблемы может стать внесение в политику безопасности организации статьи, что корпоративные ресурсы не предназначены для личных целей, и ответственность за решение обсудить личные вопросы через корпоративный канал связи полностью несет сотрудник. Таким образом, руководство компании не несет ответственности за нарушение права на тайну переписки, поскольку вся корпоративная почта принадлежит компании, и наличие в ней личных сообщений сотрудников - полностью под ответственностью сотрудников. При этом политикой безопасности следует определить перечень всех возможных средств коммуникации, а просмотр таких сообщений не будет являться нарушением права человека на тайну переписки [8].

При рассмотрении применения DLP-систем с морально - этической точки зрения, возникают другие вопросы необходимости и этичности осведомления сотрудников о внедрении в корпоративной сети организации DLP- системы и контроля трафика и содержания информационных сообщений.

С одной стороны, если персонал не знает о внедрении DLP-системы, то вероятность выявить нарушителей и каналы утечки возрастает. Однако, задача предотвратить утечку намного важнее, чем обнаружить её уже постфактум и разбираться с ее последствиями. Так же при скрытой установке, после расследования первого же инцидента, сотрудники узнают, о существовании такой системы, что может повлечь за собой ухудшение отношений в коллективе между работниками и работодателем. Отсутствие расследования инцидента и непринятие мер ответственности к нарушителю, в определенной степени лишает смысла внедрения DLP- системы. Кроме того, скрытая установка системы контроля сообщений может повлечь судебные иски и претензии со стороны персонала, в связи с неправомерностью данного вида контрольных мероприятий и нарушениями прав человека.

Открытое внедрение DLP-системы может заранее обеспечить более высокую надежность защиты информации в корпоративной системе. Когда персонал предупрежден о контроле, он более тщательно следит за отправляемой информацией, тратит меньше времени на посторонние дела. Кроме того, открытая установка системы предотвращения утечек информации меньше подрывает доверие сотрудников к работодателю, чем установка системы втайне от персонала.

Таким образом, внедрение любых DLP-систем влечет за собой ряд проблем и противоречий, связанных с соответствием нормативно - правовым актам и законодательству. Однако, корректная установка, выявление и учет всех аспектов правовой системы позволит DLP-системе стать эффективным средством защиты информации. Американский специалист по компьютерной безопасности Брюс Шнайер сказал: «Только любители атакуют машины, профессионалы же сосредоточены на людях». DLP- системы позволяют контролировать действия людей в сфере компьютерных технологий, уменьшая риски распространения конфиденциальной информации. При этом не стоит забывать, что человеческий фактор всегда был, и будет оставаться наиболее вероятной угрозой безопасности информации.

**Примечания**

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 21.07.2014) «О персональных данных» (с изм. и доп., вступ. в силу с 01.09.2015) // СПС «Консультант плюс».

2. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 12.03.2014) «О коммерческой тайне»// СПС «Консультант плюс».

3. Закон от 21.07.1993 № 5485-1(ред. от 08.03.2015) «О государственной тайне» // СПС «Консультант плюс».

4. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 13.07.2015) «О связи» (с изм. и доп., вступ. в силу с 24.07.2015)// СПС «Консультант плюс».

5. Применение DLP систем в работе с персоналом в организации // Information Security Searchinform: [электр. ресурс] URL: http://searchinform.ru/news/digest-articles/3227/ (дата обращения: 23.11.2015).

6. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СПС «Консультант плюс».

7. Валерий Васильев. Права сотрудников и безопасность корпоративных данных//Сетевая газета InfoSecurity.ru URL: http://www.infosecurity.ru/_gazeta/content/101029/art2.shtml (дата обращения: 23.11.2015).

8. Алексей Дрозд. DLP: Юридические нюансы, практические аспекты// Журнал «Персональные данные», №11(52) ноябрь 2012.

---

**Шабуров Андрей Сергеевич,** доцент, кандидат технических наук, ПНИПУ, ЭТФ, кафедра АТ, г. Пермь. E-mail: shans@at.pstu.ru

**Журилова Елена Евгеньевна,** студент, ПНИПУ, ЭТФ, кафедра АТ, г. Пермь. E-mail: Ele11485995@yandex.ru

**Shaburov Andrew,** Associate Professor, Candidate of Technical Sciences, National Research Polytechnic University, Perm. E-mail: shans@at.pstu.ru

**Zhurilova Elena,** a student Perm National Research Polytechnic University, Perm. E-mail: Ele11485995@yandex.ru