УДК 34

DOI 10.21661/r-119420

Т.В. Мавринская, А.В. Лошкарёв, Е.Н. Чуракова

DLP-СИСТЕМЫ И ТАЙНА ЛИЧНЫХ ПЕРЕПИСОК

***Аннотация**: как отмечают авторы, с каждым днем возрастает количество угроз информационной безопасности, и это требует увеличения средств (систем) информационной защиты организаций, предприятий. Существует множество средств защиты информации с различными функциональными возможностями, но основным средством предотвращения утечки информации является система Date Loss Prevention (DLP). При необходимости установления контроля за утечкой конфиденциальной информации возникает ряд вопросов соответствия принимаемых решений законодательству и нормативно-правовым актам. В данной статье рассмотрен вопрос о соответствии функциональных возможностей DLP-системы положениям и требованиям законодательства в сфере защиты семейной и личной тайны, а также соответствия Конституционному праву граждан на тайну переписки.*

***Ключевые слова**: информационная безопасность, конфиденциальная информация, утечка информации, DLP-система, защита персональных данных.*

T.V. Mavrinskaya, A.V. Loshkaryov, E.N. Churakova

DLP SYSTEM AND THE SECRET OF PERSONAL CORRESPONDENCE

***Abstract**: according to the authors, every day a number of threats to information security increases, and this requires an increase in resources (systems) of information protection of organizations and enterprises. There are many information security tools with different functionality, but the main mean of preventing information leakage is the Date Loss Prevention (DLP) system. If you need to establish control over the leak of confidential information there appear a number of questions of conformity of decisions with the legislation and regulations. This article describes the issue of compliance functionality of a DLP system the provisions and requirements of the legislation in the*

sphere of protection of family and personal secrets, as well as compliance with the Constitutional right of citizens to privacy of correspondence.

***Keywords**: information security, confidential information, information leakage, DLP system, the protection of personal data.*

В последние десятилетия XX века обозначилось значительное влияние информации на общество. С одной стороны, информация представляет ценность государства, компаний и отдельных лиц, с другой же стороны, информация является мощнейшим средством управления человеком. В связи с чем, остро встает вопрос защиты информации, так как с каждым днем возрастает число угроз информационной безопасности. Необходимость увеличения защищенности организаций, предприятий и иных учреждений стали осознавать руководители данных учреждений. Это и послужило импульсом в развитии и внедрении систем защиты информационной безопасности.

Сегодня успешность любой организации зависит во многом от информации, которой она обладает. Утечка конфиденциальной информации может нанести значительный ущерб имиджу организации, в том числе и финансовому положению, вплоть до остановки бизнес-процессов, поэтому необходимо внедрение систем предотвращения утечек конфиденциальной информации.

Один из основных способов защиты конфиденциальной информации от утечек является установление в организации режима коммерческой тайны в соответствии с Федеральным законом №98-ФЗ от 29.07.2004 «О коммерческой тайне» [2]. Введение данного режима позволяет руководителю организации определять для работников права доступа к конфиденциальной информации и ответственность за ее разглашение или утерю. В трудовом договоре, а также в уставе организации или в политике безопасности организации необходимо открыто прописать, что работодатель имеет право осуществлять контроль деятельности работника на рабочем месте, в том числе анализ корпоративной почтовой системы. На сегодняшний день такой анализ могут производить DLP-системы.

DLP-системы позволяют руководству организаций контролировать информационные потоки, выявлять внутренних недоброжелателей, отслеживать появление каналов утечки конфиденциальной информации. Данные системы производят сканирование рабочей почты, доступа в сеть Интернет, всевозможных мессенджеров, документов, отправляемых на печать в принтеры. И в процессе сканирования DLP определяет по заранее заданным критериям, является отправленная информация конфиденциальной или нет.

Однако при внедрении DLP-системы в информационную структуру организации, часто возникает вопрос о соответствии функциональных возможностей DLP-системы положениям и требованиям законодательства в сфере защиты семейной и личной тайны, а также соответствия Конституционному праву граждан на тайну переписки [6, с. 23].

Для решения данной проблемы работодателю необходимо не только технически правильно внедрить DLP-систему, но и корректно регламентировать работу с информационными системами организации. В соответствии со Статьей 10 ч. 4 №98-ФЗ от 29 июля 2004 г. «О коммерческой тайне»: «Обладатель информации, составляющей коммерческую тайну, вправе применять при необходимости средства и методы технической защиты конфиденциальности этой информации, другие, не противоречащие законодательству Российской Федерации, меры» [2]. Корпоративная почтовая система принадлежит организации, и работодатель обязан довести до работника под роспись, что использовать рабочую почту можно только для выполнения должностных обязанностей.

Работник должен знать, что организация является собственником, в том числе и интеллектуальных ресурсов, включая содержание служебной переписки. Корпоративная почтовая система создается организацией и с помощью технических средств, ей принадлежащих, соответственно использование корпоративной почты в личных целях может рассматриваться работодателем, как попытка удовлетворения личных интересов и потребностей за счет ресурсов организации.

DLP-системы имеют широкий диапазон возможностей, позволяют работодателям настраивать политику безопасности в соответствии с необходимыми

коммерческими потребностями. Правильная настройка политики безопасности DLP-систем позволяет решить проблему нарушения конституционного права работников на право тайны переписки. Под правильной настройкой понимается такая политика безопасности, при которой DLP-система самостоятельно, без участия людей, проводит сканирование почтового трафика и сортирует, какие письма относятся к личной переписке, какие письма к служебной переписке, а какие письма можно отнести к утечке конфиденциальной информации. Сканирование в таком режиме проходит по заранее заданным фильтрам, по ключевым словам, меткам и т. д. Оператор DLP-системы в данном случае не видит письма работников, так как всю работу производит программа, которая не является субъектом права. Даже если DLP-система предположила, что в письме содержится утечка конфиденциальной информации, оператор также не видит содержимое письма, а видит только информацию об отправителе, получателе, времени отправления и вердикт DLP-системы. Дальнейшие действия оператора DLP-систем зависят от принятых в организации регламентирующих документов. Описанный способ, когда DLP-система не предоставляет оператору содержимое письма, а только общую информацию о сообщении, не нарушает ни право работников на тайну переписки, ни положения законодательства.

Еще одним важным фактором решения данной проблемы является внесение пункта в политику безопасности организации о недопустимости использования корпоративной почтовой системы для решения личных вопросов. Данная мера перекладывает на работников ответственность за использование корпоративной почты для личных целей, так как почтовые ресурсы и их содержимое принадлежат организации. Однако в таком пункте необходимо прописать, что организация не имеет умысла читать переписку и не будет ей пользоваться при обнаружении.

Информирование работников о внедрении и использовании DLP-систем в информационных системах организации позволяют предотвратить утечки конфиденциальной информации. Работники, зная, что почтовый трафик подверга-

ется анализу, будут внимательнее относиться к служебной переписке, остерегаясь отправлять на внешние адреса личную и конфиденциальную информацию. Также, открытое внедрение DLP-систем позволит избежать ухудшения отношений в коллективе организации между работниками и работодателем, в отличии от тайной установки DLP-систем [1, с. 3].

176-ФЗ от 17 июля 1999 г. «О почтовой связи» определяет понятие «тайна связи»: *тайна переписки, почтовых, телеграфных и иных сообщений, входящих в сферу деятельности операторов почтовой связи, не подлежащая разглашению без согласия пользователя услуг почтовой связи* [4]. А понятие «оператор связи» определен в 126-ФЗ от 7 июля 2003 г. «О связи»: *юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии* [3]. Соответственно, организации, которые используют корпоративные почтовые системы для собственных нужд, не являются операторами связи и не обязаны обеспечивать тайну связи для почтового трафика, передаваемого корпоративной почтовой системой. Но организация является владельцем корпоративных почтовых ресурсов и информации, передаваемой этими ресурсами, что позволяет работодателю устанавливать требования по использованию этих систем и контролировать трафик с использованием DLP-систем.

Таким образом, при необходимости установления контроля за утечкой конфиденциальной информации возникает ряд вопросов соответствия принимаемых решений законодательству и нормативно-правовым актам. Решить данный вопрос может правильная установка DLP-системы, документирование требований при работе с корпоративными ресурсами, установление явного запрета на использования данных ресурсов для личных целей, уведомление работников о использовании DLP-систем. При выполнении этих условий DLP-системы становятся удобным инструментом контроля утечек конфиденциальной информации и повышают информационную безопасность организации.

Список литературы

1. Журилова Е.Е. О нормативно-правовых аспектах внедрения DLP-систем // Правовое регулирование защиты информации [Электронный ресурс]. – Режим доступа: http://www.info-secur.ru/is_17/Ghurilova.pdf

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

3. Федеральный закон от 07.07.2003 №126-ФЗ (ред. от 06.07.2016) «О связи» // СПС «Консультант плюс».

4. Федеральный закон от 17.07.1999 №176-ФЗ (ред. от 06.07.2016) «О почтовой связи» // СПС «Консультант плюс».

5. «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).

Мавринская Татьяна Владимировна – студентка Института права ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Mavrinskaya Tatyana Vladimirovna – student Institute of Law of FSBEI of HE “Samara State University of Economics”, Russia, Samara.

Лошкарёв Андрей Викторович – канд. юрид. наук, доцент кафедры гражданского и арбитражного процесса ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Loshkariov Andrey Viktorovich – candidate of juridical sciences, associate professor of the Department Civil and Arbitration process of FSBEI of HE “Samara State University of Economics”, Russia, Samara.

Чуракова Екатерина Николаевна – канд. юрид. наук, доцент кафедры гражданского и арбитражного процесса ФГБОУ ВО «Самарский государственный экономический университет», Россия, Самара.

Churakova Ekaterina Nikolaevna – candidate of juridical sciences, associate professor of the Department Civil and Arbitration process of FSBEI of HE “Samara State University of Economics”, Russia, Samara.