УДК 349.22 : 004.056.5 + 002 : 004.056 + 004.382.7.056 Вестник УрФО № 4(14)/2014. Стр. 54–57

Лаптева Т. В., Мищенко Е. Ю., Макарова П. В.

ОСОБЕННОСТИ СОСТАВЛЕНИЯ ТРУДОВЫХ ДОГОВОРОВ И СОГЛАШЕНИЙ О НЕРАЗГЛАШЕНИИ ИНФОРМАЦИИ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, НА ПРЕДПРИЯТИЯХ, ИСПОЛЬЗУЮЩИХ DLP-СИСТЕМЫ

Тема данной работы: организационные меры при использовании продуктов DLP. Широкий функционал DLP-систем позволяет собирать информацию о деятельности сотрудников на рабочем месте без их ведома, что ставит следующие цели и задачи: учесть интересы работников и работодателей и сформулировать ряд условий. Результатом работы является форма соглашения о неразглашении информации, составляющей коммерческую тайну, и трудового договора, с учетом выявленных особенностей DLP-систем, что отличает данную работу от родственных по тематике.

Ключевые слова: *информация, безопасность, защита информации, DLP-системы, трудовой договор, соглашение о неразглашении.*

Lapteva T. V., Mischenko E. Y., Makarova P. V.

FEATURES OF EMPLOYMENT CONTRACTS AND NON-DISCLOSURE AGREEMENTS WHICH COMPRISE TRADE SECRETS AT ENTERPRISES WHICH USE DLP SYSTEMS

The topic of the work is the organizational measures in the process of using DLP products. Broad functionality of DLP systems can collect information on the activities of employees on the workplace without their knowledge which establishes the following goals and objectives: to take into account the interests of employees and employers and to develop certain conditions. The result of the aforementioned work is a form of non-disclosure agreements which comprises a trade secret, as well as the employment contract based on identified features of DLP systems which distinguishes the article from related works.

Keywords: *information, security, information security, DLP systems, employment agreement, non-disclosure agreement.*

Широкое распространение DLP-систем и стремительный рост рынка данной продукции в последнее время определяет актуальность и значимость вопроса разработки на предприятии документации, регламентирующей порядок использования таких систем. Кроме того, производители таких систем заявляют, что помогают своим клиентам соблюдать законодательство, в том числе: ФЗ-98 «О коммерческой тайне», Приказ ФСТЭК России от 18.02.2013 № 21 и др.

Предотвращение утечек (англ. Data Leak Prevention, DLP) — технологии предотвращения утечек конфиденциальной информации за пределы информационной системы, а также технические устройства (программные или программно-аппаратные) для такого предотвращения утечек [1]. Примеры различных торговых марок, выпускающих продукты DLP: InfoWatch , Websense, McAfee, Symantec, Инфосистемы Джет, Zecurion, МФИ Софт, GTB. По некоторым данным объем рынка DLP-систем в 2013 году составил 2265 млн. рублей, а рост – порядка 28%.

Возможности DLP, обозначенные вендорами:

1) контроль информационных потоков, передаваемых по каналам связи: корпоративной и личной электронной почты, вебсайтов, сервисов мгновенных сообщений (в текстовом представлении, средствами АС);

2) контроль файлов на рабочих станциях и серверах: данных, хранимых на серверах, мобильных и внешних носителях, рабочих станциях, системах хранения данных (средствами АС);

3) создание снимков экрана рабочих станций: непосредственно используемой информации (графическое представление, анализ человеком и ПО);

4) запись веб-камерами в составе рабочей станции и штатными камерами видеонаблюдения (видеоинформация, анализ человеком и ПО);

5) запись аудиомикрофонами в составе рабочей станции, дополнительное оборудование (аудио, человек + ПО).

Если возникает подозрение о том, что информация покидает разрешенный периметр, срабатывает одно из трех заранее определенных правил: доставка адресату разрешается, система приостанавливает доставку до решения специалиста безопасности или доставка блокируется. Но вместе с информацией правообладателя, составляющей коммерческую тайну, в системе обрабатываются также персональные данные и общедоступная информация. Однако сведения о просмотре общедоступной информации конкретным лицом не являются общедоступными, такую информацию можно отнести к тайне личной жизни.

Для того чтобы более детально рассмотреть правовую сторону вопроса, обратимся к законодательству РФ. Во-первых, на защиту прав граждан становится Конституция РФ. Например, в ст. 23 говорится, что каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, а также на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений [2]. Во-вторых, защита прав и свобод граждан гарантируется посредством Гражданского кодекса (например, ст. 152.2) Российской Федерации, Уголовного кодекса Российской Федерации и Семейного кодекса Российской Федерации.

Статья 137 УК РФ предусматривает наказание за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Статья 138 УК РФ определяет ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан [3].

В Кодексе об административных правонарушениях тоже есть положение, а именно статья 13.11, предусматривающая ответственность за нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных). Защита информации, составляющей тайну личной или семейной жизни, обычно неразрывно связана с охраной персональных данных. В ст. 2 ФЗ-152 обозначается цель документа, а именно – обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну [4].

Теперь рассмотрим вопрос с другой стороны. Если на предприятии введен режим коммерческой тайны, обладатель информации заинтересован в её сохранности и должен принять меры для защиты, такую задачу

ставит ФЗ-149 «Об информации, информационных технологиях и о защите информации» и ФЗ-98 «О коммерческой тайне» (ст. 10).

ФЗ-149, статья 6, пункты 3–4:

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа; <…>

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами[5].

Производители DLP-систем указывают на то, что в законодательстве нет определения понятий «личная и семейная тайна» и «частная жизнь лица», используемых в статье 137 УК РФ, а значит, они могут использовать удобную для себя трактовку этого понятия.

Также производители DLP настаивают на том, что их продукт не входит в категорию средств, предназначенных для негласного получения информации [6], и на них не распространяется действие ст. 138.1 УК РФ, а значит для производства, реализации и приобретения таких систем лицензии ФСБ не нужны.

В настоящее время не опубликовано прецедентов судебной практики, связанных с использованием DLP-систем. Однако можно привести яркий пример привлечения к дисциплинарному взысканию по инциденту, в расследовании которого бы такие системы были полезны. Сотрудница турфирмы «Интерсити сервис» (холдинг KPM Group) Кира Белокрылова в течение года отправляла конфиденциальную информацию в другую туристическую компанию как со своего компьютера, так и с компьютеров других сотрудниц. Уволена по статье 81 ч. 6 Трудового кодекса – разглашение коммерческой тайны (2008 год).

Кроме того, следует обратить внимание на определение Конституционного Суда по делу Захаркиных (2005 год), где сказано, что в понятие «частная жизнь» включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер [7].

Руководство предприятия может преследовать различные цели, разворачивая DLP-систему в стенах организации:

1) предотвращение утечек коммерческой тайны путем блокирования известных каналов широко распространенными методами, снизить риск утечек;

2) облегчение расследования инцидентов разглашения информации, составляющей коммерческую тайну, за счет архивирования событий, совершаемых пользователями;

3) оценка лояльности сотрудника (выявление систематических нарушений, проступков, фактов передачи конфиденциальной информации);

4) обеспечение требований законодательства.

Обычно целью руководства организации не является тотальное увольнение сотрудников. В том случае, если руководство организации действительно хочет предотвратить утечку КТ, имеет смысл предупредить сотрудников о применяемых мерах контроля (помимо ознакомления с Положением о коммерческой тайне и Перечнем информации, составляющей коммерческую тайну).

Предлагаемое решение:

1) обозначить правила, запрещающие обработку (хранение и передачу) личной информации на корпоративных устройствах, а также использование в этих целях корпоративных сервисов;

2) предупредить о том, что в компании используются средства мониторинга и контроля выполнения правил;

3) заявить об отсутствии умысла читать личную переписку.

В таком случае работник самостоятельно делает выбор – не использовать корпоративные средства в личных целях или использовать, зная, что эта информация может оказаться доступной офицерам информационной безопасности.

Таким образом, предлагается включить в соглашение о неразглашении или трудовой договор с работником (к примеру, в раздел второй «Права и обязанности сторон») следующие пункты:

2.1. В целях охраны конфиденциальности информации Работник обязан:

2.1.1. Выполнять установленный работодателем режим коммерческой тайны.

2.1.2. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях.

2.1.3. Не разглашать информацию, составляющую коммерческую тайну, обладателями которой являются работодатель и его контрагенты, после прекращения трудового договора в течение срока, предусмотренного соглашением между работником и работодателем, заключенным в период срока действия трудового договора, или в течение трех лет после прекращения трудового договора, если указанное соглашение не заключалось.

2.2. Работник обязуется не использовать корпоративное оборудование в личных целях, в том числе для обработки, хранения и передачи личной информации.

2.3. Работодатель оставляет за собой право контролировать выполнение пунктов 2.1 и 2.2, в том числе с использованием программно-аппаратных средств мониторинга.

2.4. Использование программно-аппаратных средств мониторинга Работодателем не будет применяться для умышленного чтения личной переписки.

References

1. Wikipedia: The Free Encyclopedia [Electronic Resource], 2014. URL: https://ru.wikipedia.org/wiki/Predotvrashchenie_utechek_informatsii

2. The Constitution of the Russian Federation, 2014. URL: http://www.consultant.ru/document/cons_doc_LAW_2875/?frame=1

3. The Criminal Code of the Russian Federation as of 13.06.1996 No. 63-FZ, 2014. URL: http://www.consultant.ru/popular/ukrf/

4. Federal law as of 27.07.2006 No. 152-FZ (editorship as of 04.06.2014) 'On personal data' ,2014. URL: http://www.consultant.ru/document/ cons_doc_LAW_163964/

5. Federal law as of 27.07.2006 No. 149-FZ (editorship as of 21.07.2014) 'On information, information technologies, and information security', 2014. URL: http://www.consultant.ru/document/cons_doc_LAW_165971/

6. Prozorov A., Informatsionnaya bezopasnost' v Rossii i mire [Information Security in Russia and in the World]// 4 goryachikh yuridicheskikh voprosa pro DLP [Electronic Resource], 2014.URL: http://www.securitylab.ru/blog/personal/80na20/79635.php

7. Decision of the Constitutional Court of the Russian Federation as of 09.06.2005 No. 248-O, 2005. URL: http://sutyajnik.ru/documents/278.html

Лаптева Тамара Владимировна, студент ЮУрГУ. E-mail: tamara.lapteva@gmail.com

Мищенко Евгений Юрьевич, ст. преподаватель ЮУрГУ.

Макарова Полина Викторовна, к. п. н., доцент ЮУрГУ.

Tamara Vladimirovna Lapteva, student of South Ural State University. E-mail: tamara.lapteva@gmail.com

Evgeny Yurievich Mischenko, senior lecturer of South Ural State University.

Polina Viktorovna Makarova, Cand. Sc. Pedagogics, associate professor of South Ural State University.