Казанцева С.Ю., доцент кафедры «Экономическая безопасность, учет и право» ФГБОУ ВО «Донской государственный технический университет», Ростов-на-Дону, Россия; S-kazantseva@yandex.ru

Самойленко Ю.Ю. студент ФГБОУ ВО «Донской государственный технический университет», Россия, г. Ростов-на-Дону; Kipelov_4830@mail.ru

ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПО СРЕДСТВАМ УСТАНОВЛЕНИЯ РЕЖИМА КОММЕРЧЕСКОЙ ТАЙНЫ

Аннотация. В статье рассмотрена специфика и содержание коммерческой тайны как неотъемлемого элемента системы управления организации. Авторами обобщены основные моменты, влияющие на качество, стабильное функционирование организации, предложены пути улучшения и эффективности.

Ключевые слова: Коммерческая тайна, конфиденциальная информация, обработка персональных данных.

Kazantseva S.Yu, associate Professor of «Economic safety, accounting and law» of the «Donskoy state technical University», Rostov-on-don, Russia; S-kazantseva@yandex.ru

Samoylenko.Y.Yu student of the «Donskoy state technical University», Russia, Rostov-on-don; Kipelov_4830@mail.ru

PROTECTION OF PERSONAL DATA BY MEANS OF ESTABLISHING THE MODE OF COMMERCIAL SECRET

Abstract. The article discusses the specifics and content of commercial secrets as an integral element of the organization’s management system. The authors summarized the main points affecting the quality and stable functioning of the organization, suggested ways of improvement and efficiency.

Keywords: Trade secrets, confidential information, personal data processing.

Защита коммерческой тайны - это хорошо зарекомендовавшая себя концепция, функционально связанная с воздействием инноваций в эволюции

экономики. Начиная с 19-го века промышленная, революция побуждала законодателей формировать понятие коммерческой тайны в качестве конкретного актива, заслуживающего юридической защиты.

Из всех видов интеллектуальной собственности коммерческая тайна важна для большинства предприятий России. Коммерческая тайна существует, как на крупных, так и небольших фирмам, и охватывает многие отрасли промышленности и деятельности. И все же в понимание коммерческой тайны все еще содержится ряд пробелов.

«Информация, составляющая коммерческую тайну» – это объем данных, которые компания определяет самостоятельно, исходя из возможных угроз.

Диапазон интеллектуальных материалов, которые можно считать «коммерческой тайной», широк. Он может включать конфиденциальную деловую информацию, такую как списки клиентов фирмы, прайс-листы или маркетинговые стратегии; ноу-хау, например, факты о методах производства или процессах для достижения определенных результатов; и техническая информация, такая как чертежи, алгоритмы и химические формулы.

Сведения могут делиться на 3 ветви: научно-техническая информация, производственная информация, финансовая информация.

В таблице 1 раскрыта классификация коммерческой тайны по ветвям информации. Реальная или потенциальная коммерческая ценность подобных сведений увеличивается благодаря недоступности для третьих лиц. В отношении сведений устанавливают режим коммерческой тайны[1].

Таблица 1 – Классификация коммерческой тайны по ветвям информации.

	Коммерческая тайна	
Научно-техническая информация	**Производственная информация**	**Финансовая информация**
Характер исследовательских работ	Способы производства и технология	Состояние расчетов с торговыми клиентами
Содержание патентов и лицензий	Объем выпуска и реализации продукции	Уровень платежеспособности предприятия

Содержание рационализаторских предложений	Уровень складских запасов	Фактическое состояние рынков сбыта
Планы внедрения новых технологий и видов продукции	Планы инвестиций в новое строительство и реконструкцию производства	Сведения об эффективности экспорта и импорта
Анализ конкурентоспособности выпускаемой продукции	Методы и организация управления	Сведения о финансовом положении поставщиков, конкурентов, посредников, потребителей

Каждая компания имеет коммерческую тайну. Для некоторых это может включать списки клиентов, стратегии продуктов или конфиденциальную информацию. Для других это может быть формула или сложная и сложная методология для создания передового технологического продукта. Для всех конфиденциальная информация может представлять жизненную силу организации, которая имеет решающее значение для ее способности продавать продукты, производить продукты, получать конкурентные преимущества и пользоваться репутацией инноваций.

По своей природе коммерческая тайна не защищена так же, как традиционные формы интеллектуальной собственности. Когда происходит незаконное присвоение, другими словами утечка, организация должна доказать, что она предприняла «разумные шаги» для предотвращения кражи или злоупотребления конфиденциальной информацией.

Внедрение современных технических средств, как ничто поможет защитить весь объем информации, сохранить от несанкционированного проникновения и хищения данных, хранящихся в электронных базах данным[2]. Для сохранения и поддержания конфиденциальности от утечек, необходим целый ряд процедур, направленных на обеспечение безопасности

информации внутри компании. Хотя экономисты не проводили обширных исследований по поводу затрат фирм на защиту коммерческой тайны, но без сомнения, они являются дорогостоящими.

На рисунке 1 представлены требования к системе защиты конфиденциальной информации

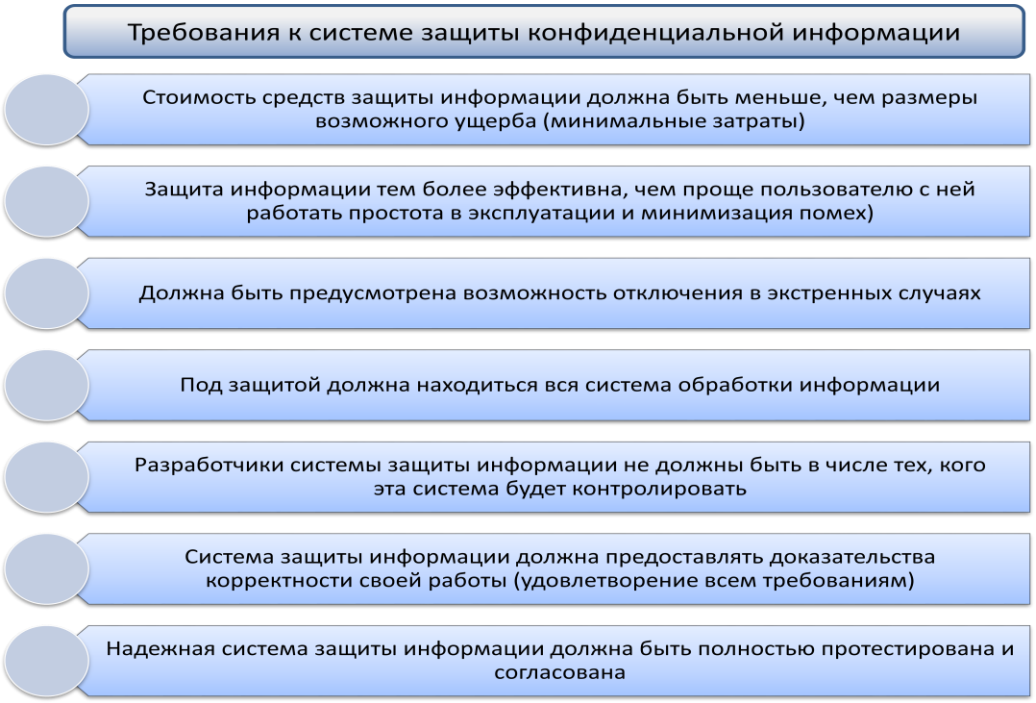

Рис. 1 – Требования к системе защиты конфиденциальной информации.

Стоит отметить, что с правовой точки зрения защита коммерческой тайны, со стороны действующего законодательства исходя из практики встает на защиту компании, что влечет за собой увольнение сотрудника только в судебном порядке по основанию «разглашение коммерческой тайны». Также ситуация может быть оспорена и в обратном направлении.

Подобные примеры подчеркивают необходимость внимательно относиться к регламентации вопросов, связанных с установлением режима коммерческой тайны. Тогда компании под силу не только защитить важные коммерческие сведения, но и возместить финансовые потери в случае инцидента, который может привести к оттоку клиентов, потере позиций в конкурентной среде и подрыве репутации.

Как показывает практика, что часть финансовых потерь любой организации напрямую связана с ее сотрудниками. Персонал – главное

достояние компании, ее «лицо», основная движущая и созидающая сила. Но не стоит забывать, что одновременно он является и источником разнообразных рисков – материальных, профессиональных, социальных.

В соответствии с Федеральным законом «О персональных данных» (или Законом о защите данных) личные данные российских граждан должны собираться и обрабатываться только с их согласия, если иное не установлено законом.

Тем не менее, нет утвержденного списка того, что - или в какой комбинации - должно считаться персональными данными. Российские юристы бесконечно спорят по этому вопросу, используя в своих аргументах определенные прецеденты или логические выводы. Обобщив все мнения, можно прийти к следующему выводу, к списку персональных данных относиться:

- ФИО
- Дата и место рождения
- Адрес
- Паспортные данные
- Семейный статус, социальный статус и статус собственности
- Доход
- Данные геолокации
- Айпи адрес
- Фото
- Ссылка на профиль в социальных сетях

Оператор данных - это объект, который выполняет определенные операции обработки данных. Операторы данных несут ответственность за нарушение прав субъектов данных в виде значительных административных штрафов, блокирование веб-сайтов, заявок и принудительное прекращение всех видов деятельности в России. В соответствии с Законом о персональных данных оператор обрабатывает данные и организует такую обработку (самостоятельно или совместно) и определяет данные для целей обработки и

список операций, применяемых к этим данным. Согласно этому определению, объект рассматривается как оператор данных не только в том случае, если он обрабатывает данные сам по себе, но также, если он доверяет третьему лицу операции обработки, когда третья сторона обрабатывает от имени оператора.

В рамках этой области субъекты персональных данных имеют право:

– узнать, обрабатываются ли их персональные данные,

– запрашивать информацию в случае обработки их данных,

– узнать цель обработки данных и используется ли она для этой цели,

– знать о третьих лицах, получающих соответствующие личные данные дома или за рубежом,

– исправление личных данных, в случае, если оно не полностью или неправильно обработано и в рамках этой области запрашивает уведомление третьим лицам, которым передаются личные данные,

– требовать удаления или удаления персональных данных и уведомлять третьих лиц, которые получили данные такого действия, в случае исчезновения причин обработки персональных данных, несмотря на то, что соответствующие данные были обработаны.

– объект к результатам обработанных анализов данных, сделанных исключительно электронными системами, если они находятся в ущерб субъектам персональных данных,

– требовать компенсацию за ущерб, в случае возникновения какого-либо ущерба из-за обработки личных данных вопреки закону.

Все действия, связанные с персональными данными, составляют обработку данных и требуют принятия конкретных предварительных мер. Например, перед обработкой данных операторы должны обеспечить, чтобы они имели законное согласие с данными, подлежащими обработке их данных, и уведомляли Роскомнадзор перед обработкой данных.

Оператор должен получить согласие субъекта данных перед обработкой. Согласие является ключевым понятием, связанным с законными операциями, помимо исключительных случаев. Наиболее распространенными случаями

являются обработка для выполнения контракта (в котором субъект данных является стороной), обработки общедоступных данных и обработки для соответствия требованиям законодательства. В Законе о персональных данных содержатся конкретные требования к содержанию, на которые субъект должен дать согласие, без предписания какой-либо конкретной формы.

На практике при нарушении установленного режима коммерческой тайны часто возникают спорные ситуации. Например, похищение из электронного почтового ящика писем, на которых отсутствовал гриф «коммерческая тайна», но имеющих важное значение, не снижает их конфиденциальной ценности. Они могут предназначаться только для внутреннего пользования и не подлежать огласке.

Организации должны соблюдать уставные обязательства по внедрению системы защиты персональных данных. По мнению различных экспертов, службы безопасности предприятия, соблюдение правовых обязательств в области защиты данных имеет важное значение. У экспертов по защите данных есть большие группы инспекторов для проведения проверки системы защиты персональных данных и применения штрафов наряду с санкциями, посредством жалобы любого пострадавшего лица.

Для этого на предприятии должно быть разработано и утверждено в соответствии с законодательством Положение, которое устанавливает порядок обработки и защиты персональных данных:

– Когда компании получают персональные данные, всем заинтересованным сторонам следует заранее сообщить о существовании системы защиты персональных данных, процесса обработки данных, целях сбора данных, получателей данных, прав доступа, исправление, аннулирование и противодействие обработке данных.

– Организации назначат лицо, ответственное за системы обработки персональных данных.

– Соблюдайте правила и положения о защите персональных данных, а также стандарты для корпоративных служб защиты персональных данных.

– обрабатывать личные данные только тогда, когда они относятся к цели, для которой они были собраны.

– Внедрить меры безопасности для служб корпоративной защиты данных.

– Модифицируйте личные данные, когда это необходимо, исправляйте неверные данные и завершайте частичные данные. Все эти изменения должны быть зарегистрированы в защищенном документе.

– Клиент имеет право запросить исправление или удаление своих персональных данных.

– Внедрить определенный набор политик для управления и обслуживания системы обработки персональных данных.

– Разработать план учебных курсов по защите персональных данных. Все специалисты отдела безопасности должны пройти обучение по защите данных.

Для этого на предприятии должно быть разработано и утверждено в соответствии с законодательством Положение, которое устанавливает порядок обработки и защиты персональных данных.

Список литературы:

1. Уваева М. Споры вокруг служебной информации // Трудовое право. 2016. N 3. С. 49–59.
2. Анашенко И. К. Режим коммерческой тайны в организации // Молодой ученый. 2016. №28. С. 617-619.
3. Шалаев А. В. «Справочник кадровика: полное практическое руководство», «ГроссМедиа», «РОСБУХ», 2016
4. Гражданское право: Учебник: в 2 т. / С. С. Алексеев, О. Г. Алексеева, К. П. Беляев и др.; под ред. Б. М. Гонгало. М.: Статут, 2016. Т. 1. 511 с.
5. Синцов Г. В., Портнова Е. В. Соотношение понятий «секрет производства», «ноу-хау» и «коммерческая тайна» // Юридический мир. 2012. N 9. С. 35–37.

6. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) «О коммерческой тайне».
7. Гладких В. И., Сбирунов П. Н. Особенности квалификации незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну // Юрист. 2012. N 5. С. 36–41.

References:

1. Uvaeva M. Disputes around proprietary information // Labor Law. 2016. N 3. P. 49–59.
2. Anashenko IK. The regime of trade secrets in the organization // Young scientist. 2016. №28. Pp. 617-619.
3. A. Shalaev, “Personnel Handbook: A Complete Practical Guide,” GrossMedia, ROSBUKH, 2016
4. Civil law: Textbook: in 2 t. / S. S. Alekseev, O. G. Alekseeva, K. P. Belyaev and others; by ed. B.M. Gongalo. M .: Statute, 2016. T. 1. 511 p.
5. Sintsov G.V., Portnova E.V. The relation of the concepts “secret of production”, “know-how” and “commercial secret” // Legal World. 2012. N 9. P. 35–37.
6. Federal Law of July 29, 2004 No. 98-ФЗ (as amended on April 18, 2017) “On Commercial Secrets”.
7. Gladkikh V.I., Sbirunov P.N. Features of the qualification of illegal receipt and disclosure of information constituting a commercial, tax or bank secret // Lawyer. 2012. N 5. P. 36–41.