

ПРОБЛЕМЫ СОВЕРШЕНСТВОВАНИЯ МЕР ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Гильманшина Алия Линатовна

студентка 2 курса магистратуры юридического факультета

Стерлитамакский филиал федерального государственного бюджетного образовательного учреждения высшего образования "Башкирский государственный университет", г. Стерлитамак

Аннотация. Высокие темпы информатизации современных технологий повышают риски уязвимостей в системах информационной безопасности организаций и используются нарушителями для несанкционированного получения персональных данных и интеллектуальной собственности. Для повышения защищенности информации предложена система комплексных мер организационно-правового характера.

Ключевые слова: персональная информация, защиты персональных данных, информатизация, современные технологии, безопасность.

В связи с широким использованием персональной информации встает вопрос о реальном состоянии защиты правового поля личности. Статья 5 Федерального закона «О персональных данных» от 27.07.2006 г. № 152-ФЗ (далее – ФЗ «О персональных данных») устанавливает принципы обработки персональной информации. Во-первых, обработка конфиденциальной информации должна ограничиваться достижением определенных и законных целей. Во-вторых, не разрешена обработка персональной информации, которая не отвечает целям ее обработки. В-третьих, содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки, т.е. обрабатываемая персональная информации не должна быть избыточной.

На основе всего вышеизложенного, включение в гражданско-правовой или трудовой договор требования обязательности предоставления избыточной персональной информации является нарушением российского законодательства. Однако законом не определен необходимый минимум персональной информации и, следовательно, не установлена юридическая ответственность. Поэтому на практике имеет место злоупотребление операторами права сбора, обработки, передачи и хранения конфиденциальных данных.

Также в п. 7 ст. 5 ФЗ «О персональных данных» установлено, что персональная информация должна храниться не дольше определенного времени, которое требуется для достижения целей ее обработки. Обрабатываемая конфиденциальная информация должна быть уничтожена либо обезличена после достижения целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим

законодательством.

Организации должны в своей деятельности руководствоваться собственными локально-нормативными актами. Например, ООО «ВЕКА» в своем регламенте установило срок хранения персональной информации клиентов в течение 75 лет. Возникает законное сомнение в необходимости хранения данных субъектов персональной информации в течение всей их жизни. Отсюда возникает необходимость в ограничении срока хранения персональных данных и внесение обязательной процедуры их уничтожения.

Обработка персональной информации осуществляется только с письменного согласия субъекта на обработку его личных данных согласно ст. 6 ФЗ «О персональных данных». Однако субъекту персональной информации в организации не предоставляются гарантии защиты его персональной информации.

В нормативном акте «Требования к защите персональных данных при их обработке в информационных системах персональных данных» (утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119) сказано, что обеспечение безопасности персональных данных при их обработке в информационной системе возлагается на оператора этой системы или на лицо, которое осуществляет обработку персональной информации по поручению оператора.

Информационная система – это совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств. Оператором может являться государственный орган, муниципальный орган, юридическое или физическое лицо, которое самостоятельно или совместно с другими лицами организует и (или) осуществляет обработку персональной информации.

Механизм защиты оператором персональной информации субъектов позволяет выделить три типа актуальных угроз:

1. угрозы 1-го типа, которые актуальны при наличии недокументированной возможности в системном программном обеспечении, которое используется в информационной системе;
2. угрозы 2-го типа, которые актуальны при отсутствии недокументированной возможности в прикладном обеспечении, которое используется в информационной системе;
3. угрозы 3-го типа, которые актуальны при отсутствии недокументированной возможности в системном и прикладном обеспечении, которое используется в информационной системе;

Информационные системы классифицируются по типу персональной информации и по типу субъектов персональной информации:

1. обрабатывающие специальные категории персональных данных;

2. обрабатывающие биометрические персональные данные;
3. обрабатывающие общедоступные персональные данные;
4. обрабатывающие иные категории персональных данных;
5. обрабатывающие персональные данные сотрудников оператора.

Уровень обеспечения защиты определяется с учетом выбранного типа угроз, категории персональных данных и количества субъектов. Настоящие требования устанавливают четыре уровня обеспечения защиты персональной информации, которыми обеспечиваются условия информационной защиты каждого из уровней.

Из этого следует, что любая организация должна ознакомить субъекта персональной информации с уровнем защиты его личных данных и условиями обеспечения информационной защиты данных. Для этой цели организации на локально-нормативном уровне необходимо разработать документ о информационной безопасности персональной информации.

Список литературы:

1. Федеральный закон от 27 ноября июля г. № 152-ФЗ «О персональных данных» (с посл. изм. и доп. от 31 декабря 2017 г. № 498-ФЗ) // Официальный интернет-портал правовой информации [Электронный ресурс]. URL:<http://www.pravo.gov.ru/> (дата обращения: 17.08.2019).
2. Постановление Правительства РФ от 01 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" // Официальный интернет-портал правовой информации [Электронный ресурс]. URL:<http://www.pravo.gov.ru> (дата обращения: 17.08.2019).
3. Парфенов Н. П., Стахно Р. Е. Оптимизация требований к обработке персональных данных // European Science. 2016. № 11 (21). С. 25-28.
4. Стахно Р.Е., Домбровская Л.А., Яковлева Н.А. Современные подходы к защите информации, методы, средства и инструменты защиты // Наука, техника и образование. 2016. № 4 (22). С.16-19.