Приложение 3
к протоколу заседания
Единой экспертной комиссии
по вопросам реализации мероприятий
по обработке и защите персональных данных
от 02.08.2012 №3

Политика в отношении обработки персональных данных

Политика в отношении обработки персональных данных является документом, определяющим основные направления осуществления обработки персональных данных.

Необходимость разработки данного документа обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов при обработке персональных данных.

Настоящая Политика определяет основные принципы и задачи, а также общую стратегию построения системы защиты персональных данных. Данная Политика разработана в соответствии с системным подходом к обеспечению информационной безопасности.

Обработка персональных данных в основана на следующих принципах:

- осуществления на законной и справедливой основе;

- соответствия целей обработки персональных данных полномочиям;

- соответствия содержания и объема обрабатываемых персональных данных целям обработки персональных данных;

- достоверности персональных данных, их актуальности и достаточности для целей обработки, недопустимости обработки избыточных по отношению к целям сбора персональных данных;

- ограничения обработки персональных данных при достижении конкретных и законных целей, запретом обработки персональных данных, несовместимых с целями сбора персональных данных;

- запрета объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

- осуществления хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

В соответствии с принципами обработки персональных данных определены цели обработки персональных данных:

для исполнения условий трудового договора и осуществления прав и обязанностей в соответствии с законодательством, регулирующим трудовые правоотношения;

для принятия решений по обращениям физических лиц, персональные данные которых обрабатываются в связи с оказанием муниципальных услуг и осуществлением муниципальных функций.

Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных, с позиции комплексного применения технических средств защиты и организационных мер.

Применение технических средств защиты и организационных мер призваны обеспечить:

- конфиденциальность информации (защита от несанкционированного ознакомления);

- целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

- доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

Организационные меры предусматривают создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) организационно-распорядительных документов:

Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

Политика служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности, а также нормативных и методических документов, обеспечивающих ее реализацию.

Под информационной безопасностью персональных данных понимается защищенность персональных данных и обрабатывающей их инфраструктуры от любых случайных или намеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам персональных данных) или инфраструктуре. Основной целью информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к предотвращению таких воздействий.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Для достижения основной цели система безопасности персональных данных в информационной системе персональных данных (далее - ИСПДн) должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные в установленным порядке пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИСПДн;

б) средствам вычислительной техники ИСПДн;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

- регистрацию действий пользователей при использовании защищаемых ресурсов ИСПДн в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

- защиту персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

- своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

Структура, состав и основные функции системы защиты персональных данных определяются исходя из класса ИСПДн.

В соответствии с приказом ФСТЭК России, ФСБ России и Минсвязи России от 13 февраля 2008 г. №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» осуществлена классификация ИСПДн.

Классификация ИСПДн проведена в следующей последовательности: комиссией составлен акт классификации ИСПДн, для разработки требований по

обеспечению безопасности и внедрения системы обеспечения безопасности персональных данных разработана типовая модель угроз на основе нормативно-методического документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

В соответствии с нормативным методическим документом ФСТЭК России «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» разрабатывается и внедряется комплекс мер по защите и обеспечению безопасности персональных данных.

Создана и функционирует Единая экспертная комиссия по вопросам реализации мероприятий по обработке и защите персональных данных, являющаяся постоянно действующим коллегиальным органом, образованным в целях подготовки предложений и реализации мероприятий по обработке и защите персональных данных в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, регламентирующими работу с персональными данными, и соглашениями на обработку персональных данных.

Должностные обязанности работников, допущенных к обработке персональных данных, установлены в должностных инструкциях, руководствах пользователей. Обеспечение конфиденциальности обрабатываемых персональных данных является обязательным требованием для всех работников, допущенных к обработке персональных данных. Все лица, допущенные к работе с персональными данными, должны подписать обязательство о соблюдении режима конфиденциальности персональных данных.

Персональные данные поступают при приеме новых сотрудников, заключении договоров, проведении собеседований, при принятии решений по обращениям физических лиц, персональные данных которых обрабатываются в связи с оказанием муниципальных услуг и осуществлением муниципальных функций, а также в иных случаях. Работники, осуществляющие оформление

документов, обязаны получать в установленных случаях согласие субъектов персональных данных обработку.

Лица, виновные в нарушении требований законодательства в области обработки персональных данных, несут ответственность в соответствии законодательством Российской Федерации.