МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ОБРАЗОВАНИЮ

ПИСЬМО от 29 июля 2009 г. №17-110

Об обеспечении защиты персональных данных

В соответствии с письмами Роскомнадзора от 23.06.2009 №07-2/6639 и Рособразования от 03.09.2008 №17-02-09/185 напоминаем, что информационные системы персональных данных, созданные после вступления в действие Федерального закона Российской Федерации от 26.07.2006 №152-ФЗ «О персональных данных», должны соответствовать требованиям данного закона. Ранее созданные информационные системы должны быть приведены в соответствие с требованиями закона не позднее 1 января 2010 года.

Лица, виновные в нарушении требований закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Контроль за соблюдением законодательства о персональных данных осуществляют территориальные органы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзора).

В соответствии со статьей 9 Федерального закона Российской Федерации от 26.07.2006 №152-ФЗ обработка персональных данных должна осуществляться с письменного согласия субъектов персональных данных или их законных представителей. Письменное согласие в виде анкеты, заполняемой и подписываемой каждым абитуриентом, учащимся и работником учреждения, должно включать:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) срок, в течение которого действует согласие, а также порядок его отзыва по инициативе субъекта персональных данных.

В целях автоматизации обработки персональных данных в анкетах рекомендуется дополнительно указывать внутренний идентификационный номер (личный код) субъекта персональных данных, присваиваемый на весь период обучения или работы. Это позволит обезличить базы данных, если в них не содержатся иные персональные данные, и существенно сократить затраты на защиту информации.

Защита персональных данных должна осуществляться в соответствии с постановлениями Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Информация об основных нормативно-методических документах и требованиях по организации защиты персональных данных прилагается.

Н.И.БУЛАЕВ

Приложение

Информация об основных нормативно-методических документах и требованиях по организации защиты персональных данных

Законодательством Российской Федерации ответственность за надлежащую защиту персональных данных возлагается на организации, в которых персональные данные обрабатываются. Уполномоченным органом по контролю за соблюдением законодательства о персональных данных является Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).
Роскомнадзор проводит плановые (целевые, комплексные) проверки, а также проверки по жалобам и обращениям физических и юридических лиц. Проверки систем защиты персональных данных могут также осуществляться ФСТЭК России или ФСБ России при проведении контроля систем защиты конфиденциальных данных или использования криптосредств. При обнаружении неправомерных действий с персональными данными их обработка должна быть прекращена до устранения выявленных нарушений.

Нарушение законодательства о персональных данных в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных» (статья 24) влечет за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность, налагаемую в судебном порядке.

1. Законодательство о защите персональных данных

Под персональными данными (ПД) понимают любую информацию, относящуюся к определенному или определяемому на основании такой информации физическому лицу (субъекту ПД), в том числе: фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание такой обработки.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без наличия таких средств.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Трансграничная передача персональных данных - передача персональных данных оператором через государственную границу Российской Федерации.

В целях защиты прав граждан на неприкосновенность частной жизни, личной и семейной тайны в последние годы принят ряд законодательных актов. В настоящее время законодательно-нормативная база по персональным данным включает:

Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (14 глава, с изменениями и дополнениями);

Федеральный закон от 19.12.2005 №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

Федеральный закон Российской Федерации от 27.07.2006 №152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Постановление Правительства Российской Федерации от 06.07.2008 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»;

Постановление Правительства Российской Федерации от 15.08.2006 №504 «О лицензировании деятельности по технической защите конфиденциальной информации»;

Постановление Правительства Российской Федерации от 16.03.2009 №228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций»;

Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;

Приказ Россвязькомнадзора от 17.07.2008 №08 «Об утверждении образца формы уведомления об обработке персональных данных»;

Приказ Россвязькомнадзора от 18.02.2009 №42 «О внесении изменений в Приказ Россвязькомнадзора от 17 июля 2008 г. №8 «Об утверждении образца формы уведомления об обработке персональных данных».

Обеспечение безопасности персональных данных должно осуществляться в соответствии с методическими документами ФСТЭК России (документы ДСП):

«Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года;

«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;

«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года;

«Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 года.

Для получения перечисленных документов для служебного пользования можно обратиться во ФСТЭК России.

Использование криптосредств для обеспечения безопасности персональных данных должно осуществляться в соответствии с:

Приказом ФСБ России от 09.02.2005 №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации»;

Постановлением Правительства Российской Федерации от 29.12.2007 №957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»;

Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации (ФСБ России, от 21.02.2008 №149/54-144);

Типовыми требованиями по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России, от 21.02.2008 №149/6/6-622).

На основании указанных выше документов всеми организациями и физическими лицами на территории Российской Федерации должен обеспечиваться требуемый уровень безопасности персональных данных (в

действующих информационных системах - не позднее 01.01.2010). Лица, виновные в нарушении требований, несут предусмотренную законодательством Российской Федерации ответственность.

2. **Порядок обработки персональных данных, осуществляемой без использования средств автоматизации**

Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с законодательством Российской Федерации и «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства Российской Федерации от 15.09.2008 №687.

Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации (при их наличии).

Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных были:

- определены места хранения персональных данных (материальных носителей) и установлен перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

- обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях;

- соблюдены условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливается оператором в соответствии с требованиями, предъявляемыми указанными правовыми актами.

3. Основные обязанности операторов информационных систем, обрабатывающих персональные данные

Операторы обязаны обеспечивать защиту персональных данных во внедряемых информационных системах с момента их ввода в эксплуатацию.

В отношении действующих информационных систем, обрабатывающих персональные данные, операторы обязаны провести их классификацию с оформлением соответствующего акта, реализовать до 01.01.2010 г. комплекс мер по защите персональных данных в соответствии с перечисленными правовыми актами и методическими документами в виде системы защиты персональных данных, провести оценку соответствия информационной системы персональных данных требованиям безопасности в форме сертификации (аттестации) или декларирования соответствия.

4. Порядок проведения (или уточнения) классификации информационных систем персональных данных

Постановление Правительства Российской Федерации от 17.11.2007 №781 возлагает обязанность классификации информационных систем персональных данных и задачу обеспечения их безопасности на оператора персональных данных, а разработку методов и способов защиты персональных данных в информационных системах - на ФСТЭК России и ФСБ России.

Классификация информационных систем персональных данных осуществляется оператором в соответствии с Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных» в зависимости от категории обрабатываемых данных и их количества.

Установлены следующие категории персональных данных (ПД):

Категория 1 - ПД, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

Категория 2 - ПД, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД, относящихся к категории 1;

Категория 3 - персональные данные, позволяющие идентифицировать субъекта ПД;

Категория 4 - обезличенные и (или) общедоступные персональные данные.

Информационные системы персональных данных подразделяются на типовые и специальные. К типовым системам относятся системы, в которых

требуется обеспечить только конфиденциальность персональных данных. Все остальные системы относятся к специальным.

В зависимости от последствий нарушений заданной характеристики безопасности персональных данных типовой информационной системе присваивается один из классов:

класс 1 (К1) - информационные системы, для которых нарушения могут привести к значительным негативным последствиям для субъектов персональных данных;

класс 2 (К2) - информационные системы, для которых нарушения могут привести к негативным последствиям для субъектов персональных данных;

класс 3 (К3) - информационные системы, для которых нарушения могут привести к незначительным негативным последствиям для субъектов персональных данных;

класс 4 (К4) - информационные системы, для которых нарушения не приводят к негативным последствиям для субъектов персональных данных.

Класс типовой информационной системы определяется оператором в соответствии с таблицей, приведенной в Приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 №55/86/20.

Класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных по результатам анализа исходных данных в соответствии с приведенными выше методическими документами ФСТЭК России.

В случае выделения в составе информационной системы подсистем, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий наиболее высокому классу входящих в нее подсистем. Вследствие этого интегрированные информационные системы, как правило, подпадают под классы К1 и К2 и требуют больших затрат на защиту персональных данных. Защита систем упрощается, если сложная система сегментирована на несколько отдельных, не связанных друг с другом систем, различных по целям и регламентам обработки персональных данных.

Результаты классификации информационных систем оформляются соответствующим актом оператора. Класс информационной системы может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;

- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Устанавливается следующий порядок оценки соответствия степени защищенности информационных систем требованиям безопасности:

- для информационных систем 1 и 2 класса соответствие степени защищенности требованиям безопасности устанавливается путем обязательной сертификации (аттестации);

- для информационных систем 3 класса соответствие требованиям безопасности подтверждается путем сертификации (аттестации) или (по выбору оператора) декларированием соответствия, проводимым оператором персональных данных;

- для информационных систем 4 класса оценка соответствия не регламентируется и осуществляется по решению оператора персональных данных.

Операторы обязаны при обработке персональных данных принимать требуемые организационные и технические меры, в том числе при необходимости использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Система защиты персональных данных должна строиться только на основе сертифицированных ФСТЭК России и ФСБ России средствах защиты (технических, программных, программно-аппаратных и криптографических).

Без наличия соответствующих лицензий проведение мероприятий по защите персональных данных возможно только для информационных систем класса К3, а также для информационных систем класса К4.

Для проведения собственными силами мероприятий по обеспечению безопасности персональных данных для специальных информационных систем, систем 1 и 2 класса и распределенных (например, подключенных к Интернет) систем 3 класса операторы обязаны в установленном порядке получить лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Для применения криптографических средств защиты персональных данных (в том числе для изготовления ключей или сертификатов), в зависимости от планируемых действий, потребуются различные лицензии ФСБ России, регламентирующие работы в области криптографической защиты информации.

5. Основные мероприятия по обеспечению безопасности персональных данных в учреждениях образования

Исходя из требований законодательства образовательным учреждениям в течение 2009 года необходимо:

1. Определить (или уточнить) состав и категории обрабатываемых персональных данных;

2. Осуществить (или уточнить) классификацию действующих информационных систем, обрабатывающих персональные данные;

3. Провести необходимые организационные и технические мероприятия для обеспечения защиты:

- персональных данных, обрабатываемых без использования средств автоматизации;

- информационных систем, обрабатывающих персональные данные.

4. Декларировать соответствие или провести аттестационные (сертификационные) испытания информационных систем, обрабатывающих персональные данные.

Мероприятия по обеспечению безопасности персональных данных осуществляются на основе законодательства Российской Федерации, нормативных и методических документов.

В части предварительных организационных мероприятий по защите персональных данных всем подведомственным Рособразованию учреждениям и организациям следует:

- определить перечень, цели и порядок обработки персональных данных;

- назначить ответственных за работу с персональными данными;

- подготовить должностные инструкции сотрудников, обрабатывающих персональные данные;

- обеспечить размещение и охрану средств хранения и обработки персональных данных.

Для информационных систем классов К1 и К2 дополнительно потребуется принять предусмотренные методическими документами ФСТЭК России и ФСБ России меры по защите информации от утечки по техническим каналам.

6. Порядок проведения аттестационных (сертификационных) испытаний

Аттестационные (сертификационные) испытания проводятся организациями, имеющими необходимые лицензии ФСТЭК России. При этом под аттестацией понимают комплекс мер, позволяющих привести информационную систему в соответствие с требованиями по безопасности информации к заявленному классу, изложенными в нормативно-методических документах ФСТЭК России.

Аттестационные (сертификационные) испытания содержат в себе анализ уже имеющихся на объекте информационных систем персональных данных, а также вновь принятых решений по обеспечению безопасности информации и включают проверку:

- организационно-режимных мероприятий по обеспечению защиты информации;

- защищенности информации от утечек по техническим каналам (ПЭМИН);

- защищенности информации от несанкционированного доступа.

По результатам аттестационных испытаний принимается решение о выдаче «Аттестата соответствия» информационной системы заявленному классу по требованиям безопасности информации. Аттестат выдается сроком на 3 года.

7. Декларирование соответствия

Декларирование соответствия - это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России.

Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии.

В случае проведения декларирования на основе собственных доказательств оператор самостоятельно формирует комплект документов, таких как техническая документация, другие документы и результаты собственных исследований, послужившие мотивированным основанием для

подтверждения соответствия информационной системы персональных данных всем необходимым требованиям, предъявляемым к классу К3.

Независимо от используемой формы подтверждения соответствия оператор может также предоставить протоколы испытаний, проведенных в исследовательской лаборатории.

Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны имеют одинаковую юридическую силу. Также они имеют действие, аналогичное действию сертификата (аттестата) соответствия, и также действительны на территории всей страны и стран, признающих разрешительные документы системы ГОСТ Р в течение всего срока действия.

Декларация о соответствии оформляется на русском языке и должна содержать:

- наименование и местонахождение заказчика;

- информацию об объекте подтверждения соответствия, позволяющую идентифицировать этот объект, класс ИС ПД;

- наименование документов, на соответствие требованиям которых подтверждается ИС ПД;

- указание на схему декларирования соответствия;

- заявление заказчика о принятии им мер по обеспечению соответствия продукции необходимым требованиям;

- сведения о документах, послуживших основанием для подтверждения соответствия продукции требованиям;

- срок действия декларации о соответствии.

8. Заключение

Для классификации и защиты информационных систем персональных данных образовательные учреждения, не располагающие необходимыми специалистами и лицензиями, могут обратиться на договорных условиях за методической и консультационной поддержкой в организации, имеющие соответствующие лицензии.

Перечень органов (организаций) по аттестации Системы сертификации средств защиты информации по требованиям безопасности информации, а

также Государственный реестр сертифицированных средств защиты информации размещены на сайте ФСТЭК России.

Специализированным организациям могут быть поручены:

1. Методическая поддержка и консультирование при проведении сегментирования интегрированных информационных систем, определении состава и классификации информационных систем, обрабатывающих персональные данные.

2. Консультирование и помощь в формировании перечня организационно-технических мероприятий, необходимых для создания системы защиты информационных систем, обрабатывающих персональные данные.

3. Консультирование при подготовке декларации соответствия для систем класса К3.

4. Аудит информационных систем персональных данных, подбор и установка необходимых технических средств защиты информации для систем классов К2 и К1, а также распределенных информационных систем класса К3.

5. Подготовка, проведение аттестационных испытаний информационных систем классов К2 и К1 с выдачей Аттестата соответствия.

При использовании перечисленных нормативно-методических документов по защите персональных данных необходимо иметь в виду, что регулирующими органами могут вноситься уточнения и разъяснения, которые должны приниматься к исполнению всеми операторами информационных систем, обрабатывающих персональные данные.