учителя и ученика, изменение деловых отношений всего коллектива. Введение систематизированной структуры управления ОУ ведет к изменению в структуре управления и руководства.

Организационные и технические меры защиты персональных данных, обрабатываемых с использованием средств автоматизации

Комелина Елена Витальевна (elena-komelina@yandex.ru)

ГОУВПО «Марийский государственный университет», г. Йошкар-Ола

Аннотация

В данной статье приводится перечень нормативных и организационных документов, необходимых для формирования нормативно-правовой базы для работы с персональными данными в учреждении образования. Рассматриваются правила обработки и обеспечения конфиденциальности персональных данных, организационные и технические меры защиты персональных данных.

Государства – члены Совета Европы – с целью обеспечения на территории каждой из сторон уважения прав и основных свобод каждого человека независимо от его гражданства или места жительства и в особенности его права на неприкосновенность личной сферы в связи с автоматической обработкой касающихся его персональных данных приняли Конвенцию «О защите физических лиц при автоматизированной обработке персональных данных» ETS-108 (Страсбург, 28 января 1981 г.) (далее Конвенция).

Российская Федерация ратифицировала Конвенцию в 2005 году. Ратификация обязывает государство принять необходимые меры для того, чтобы основные принципы защиты данных, изложенных в Конвенции, были реализованы в ее национальном праве.

С целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных в соответствии с Конвенцией Совета Европы был принят Федеральный закон №152-ФЗ «О персональных данных» от 27.07.2006.

Данным законом, главой 14 Трудового кодекса Российской Федерации от 30 декабря 2001 г. № 197-ФЗ, постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 установлены правила в отношении порядка обработки и обеспечения конфиденциальности персональных данных, как собственных работников, так и сторонних физических лиц, персональные данные которых обрабатываются в организации.

Закон был принят на фоне абсолютной незащищенности персональной информации и постоянных публичных утечек персонифицированных баз данных, что нарушает конституционные права граждан и несет ущерб деловой репутации организаций, обладающих такой информацией.

В сферу действия Федерального закона № 152-ФЗ «О персональных данных» попали все юридические и физические лица, осуществляющие получение и обработку персональных данных, от которых требуется обеспечение конфиденциальности указанной информации. К персональным данным по закону относятся фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация о физическом лице.

За невыполнение требований указанных правовых актов, а также нормативных документов ФСБ России и ФСТЭК России по вопросам обработки персональных данных предусмотрена административная и уголовная ответственность. Возможны также гражданские иски к организации, принудительное приостановление или прекращение обработки персональных данных в организации, при определенных условиях возможно приостановление действия или аннулирование лицензий.

Персональные данные относятся к категории конфиденциальной информации, предполагающей отсутствие свободного доступа к ней и наличие эффективной системы ее защиты. Включение персональных данных в разряд конфиденциальных сведений направлено на предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в личную жизнь гражданина.

Многие руководители ОУ до сих пор не вполне ясно представляют себе, что конкретно нужно делать для защиты персональных данных в соответствии с требованиями Федерального закона № 152 от 27.07.2006 года «О персональных данных». Такая ситуация вызвана отсутствием практики применения норм Закона в проектах по обеспечению защиты персональных данных.

Основные требования по защите персональных данных общеизвестны:

– Закон «О персональных данных» предписывает в обязательном порядке обеспечить соответствующую защиту персональных данных, обрабатываемых в учреждении;

– установлен предельный срок выполнения требований для информационных систем ПДн, созданных до дня вступления в силу Закона «О персональных данных»;

– вновь создаваемые и вводимые в эксплуатацию информационные системы персональных данных должны соответствовать требованиям Закона «О персональных данных»;

– за неисполнение требований предусмотрены различные виды ответственности.

Перечень организационных и технических мероприятий также определен:

– уведомление уполномоченного органа по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных;

– разработка документов, регламентирующих обработку персональных данных в организации;

– создание системы защиты персональных данных, в т. ч. выполнение требований по инженерно-технической защите помещений;

– аттестация ИСПДН (аттестация или декларирование соответствия информационных систем персональных данных (ИСПДн) требованиям безопасности информации);

– повышение квалификации сотрудников в области защиты персональных данных.

Необходимо принять ряд мер, от которых зависит дальнейший план действий по выполнению требований законодательства.

1. Необходимо установить перечень персональных данных, обрабатываемых в ОУ.

2. Уточнить список лиц, имеющих доступ к персональным данным, а также определить источники получения персональных данных и способов их обработки.

3. Назначить ответственного сотрудника для рассмотрения всех вопросов, связанных с исполнением Закона «О персональных данных» в учреждении, а для больших ОУ может быть оправдано создание специальной рабочей группы.

4. Выявить информационные системы, в которых осуществляется обработка персональных данных (ИСПДн).

5. Определить состав и объем обрабатываемых персональных данных.

6. Провести предварительную классификацию информационных систем ПДн.

7. Проанализировать полученные результаты и определить способы защиты персональных данных.

После проведения предварительного анализа информационных ресурсов образовательного учреждения можно получить представление о состоянии информационных ресурсов в части обработки персональных данных (перечень и характеристики обрабатываемых ПДн), осознать масштаб сложности решаемых задач и определить дальнейшие шаги по выполнению требований Закона «О персональных данных».

Закон «О персональных данных» разрешает вести обработку персональных данных без подачи уведомления в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных в следующих случаях:

– если ОУ обрабатывает персональные данные сотрудников, которых связывают с учреждением трудовые отношения;

– при наличии договора с субъектом персональных данных, на основании которого персональные данные не распространяются и не предоставляются третьим лицам без согласия субъекта персональных данных и используются учреждением исключительно для исполнения указанного договора;

– если персональные данные относятся к членам общественного объединения или религиозной организации, действующими в соответствии с законодательством РФ, при условии, что персональные данные не будут распространяться без письменного согласия субъектов персональных данных;

– если персональные данные являются общедоступными;

– если персональные данные включают в себя только фамилии, имена и отчества субъектов персональных данных;

– если персональные данные необходимы для однократного пропуска на территорию предприятия;

– персональные данные включены в информационные системы персональных данных, имеющих статус федеральных автоматизированных информационных систем, а также государственных информационных систем, созданных в целях защиты безопасности государства и общественного порядка;

– персональные данные обрабатываются без использования средств автоматизации.

Во всех остальных случаях учреждение обязано подать уведомление в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) о своем намерении осуществлять обработку персональных данных. На основании уведомления организация регистрируется в реестре операторов, осуществляющих обработку персональных данных.

Комплекс мероприятий по обеспечению защиты персональных данных состоит из организационных и технических мер защиты информации.

Организационные меры по защите персональных данных включают в себя разработку организационно-распорядительных документов, регламентирующих весь процесс получения, обработки, хранения, передачи и защиты персональных данных, например:

– «Положение об обработке персональных данных сотрудников»;

– «Положение об обработке персональных данных обучающихся и воспитанников»;

– «Положение по защите персональных данных»;

– «Регламент взаимодействия с субъектами персональных данных»;

– «Регламент взаимодействия при передаче персональных данных третьим лицам»;

– «Инструкции администраторов безопасности персональных данных»;

– «Инструкции пользователей по работе с персональными данными», а также перечень мероприятий по защите персональных данных:

- определение круга лиц, допущенного к обработке персональных данных;
- организация доступа в помещения, где осуществляется обработка ПДн;
- разработка должностных инструкций по работе с персональными данными;
- установление персональной ответственности за нарушения правил обработки ПДн;
- определение продолжительности хранения ПДн и т. д.

Меры организационного характера осуществляются независимо от того, нужно подавать уведомление в Роскомнадзор или нет, обработка ПДн осуществляется с использованием средств автоматизации или без использования таких средств. Реализация организационных мер защиты информации осуществляется с учетом категорий персональных данных – чем выше категория, тем выше требования их защиты.

Технические меры защиты информации предполагают использование программно-аппаратных средств защиты информации. При обработке ПДн с использованием средств автоматизации применение технических мер защиты является обязательным условием, а их количество и степень защиты определяется в процессе предварительного обследования информационных ресурсов ОУ.

Технические средства защиты информации делятся на два основных класса:

– средства защиты информации от несанкционированного доступа;

– средства защиты информации от утечки по техническим каналам.

В отличие от организационных мер, техническая защита информации является сложным и трудоемким делом, при выполнении которого требуется соблюдать определенные условия. Для выполнения работ по технической защите конфиденциальной информации требуется:

– обследование информационных ресурсов учреждения в соответствии с методическими рекомендациями ФСТЭК (определение перечня ПДн, подлежащих защите), определение состава и структуры каждой информационной системы ПДн (ИСПДн), анализ уязвимых звеньев и возможных угроз безопасности ПДн, оценка ущерба от реализации угроз безопасности ПДн, анализ имеющихся в распоряжении мер и средств защиты ПДн);

– на основании проведенного обследования осуществляется обоснование требований по обеспечению безопасности ПДн (разработка модели угроз и модели нарушителя безопасности ПДн; определение класса информационных систем ПДн, при необходимости обосновывается использование средств шифрования);

– проведение работ по проектированию, созданию и вводу в эксплуатацию системы защиты ПДн (разработка перечня мероприятий по защите ПДн в соответствии с выбранным классом ИСПДн; согласование документов с регуляторами; разработка технического задания на создание системы защиты ПДн; развертывание и ввод в эксплуатацию системы защиты ПДн);

– аттестация (сертификация) информационных систем ПДн по требованиям безопасности информации (для ИСПДн 1-го и 2-го классов требуется аттестация соответствия требованиям информационной безопасности; сертификация средств защиты информации). Работы по аттестации (сертификации) выполняются при наличии соответствующих лицензий.

На основании методического документа ФСТЭК «Рекомендации по обеспечению безопасности ПДн при их обработке в ИСПДн» в обязательном порядке разрабатываются следующие документы:

– «Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн»;

– «Требования по обеспечению безопасности ПДн при обработке в ИСПДн»;

– «Должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн»;

– «Рекомендации по использованию программных и аппаратных средств защиты информации».

В «Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн» обязательно включаются разделы по контролю эффективности защиты информации в компании, об организации режима безопасности помещений, где осуществляется работа с ПДн, хранение и уничтожение носителей ПДн.

После изучения вопроса и понимания того, что выполнять работы необходимо, каждый руководитель задает себе следующий вопрос: можно ли самостоятельно выполнить требования законодательства или воспользоваться услугами специализированных организаций?

Если обработка персональных данных в учреждении осуществляется без использования средств автоматизации (неавтоматизированная обработка), обеспечение защиты ПДн вполне реализуемо собственными силами. При обработке ПДн с использованием средств автоматизации необходимо оценить сложность и масштабность работ, взвесить все положительные и отрицательные стороны того или иного подхода и принять оптимальное решение по выбору специализированной организации как исполнителя проекта.

Меры организационного характера в образовательных учреждениях Республики Марий Эл были проведены в срок и завершены к середине 2009 года.

С целью организации защиты информации от несанкционированного доступа и от утечки информации по техническим каналам был разработан и реализован курс повышения квалификации для системных администраторов.

Использование автоматизированной информационной системы в деятельности заместителя директора по учебно-воспитательной работе

Князева Ольга Владимировна (ol.knyazeva@yandex.ru)

ФГОУ СПО «Пермский химико-технологический техникум», г. Пермь

Аннотация

Информационная система учета часов педагогической нагрузки создана для секретаря учебной части, что позволяет регулярно отслеживать и вести учет количества часов педагогической нагрузки, проведенных за любой период времени у конкретного преподавателя, в конкретной учебной группе, значительно сократить время на обработку информации, уменьшить затраты времени на поиск необходимой информации, улучшить качество контроля.

На современном этапе развития образовательного процесса невозможно представить работу учебной части, организующей рабочий процесс в образовательном учреждении, без применения в работе компьютера и информационных технологий.

На сегодняшний день автоматизация документооборота в образовательном учреждении так же необходима, как автоматизация бухгалтерского учета в середине девяностых годов. Причин этому много. Во-первых, информацию необходимо обрабатывать как можно быстрее и качественнее, подчас