Приложение 2

УТВЕРЖДЕНО
Председатель
Комитета образования
С.Е. Поздеева
Распоряжением
№ ___ от _____2010г.

Алгоритм организации защиты персональных данных

С учетом требований действующего законодательства можно сформулировать следующий алгоритм действий по организации защиты персональных данных в образовательном учреждении.

1. Определение состава и категории обрабатываемых персональных данных

Необходимо определиться с субъектами персональных данных, объемом персональных данных учащихся (и их родителей, законных представителей), необходимых для обеспечения образовательного процесса, объемом персональных данных работников, необходимых образовательному учреждению как работодателю и в связи с задачами управления системой образования, ставящимися органами управления образованием.

2. Инвентаризация системы обработки персональных данных в учреждении

На этой стадии необходимо проанализировать все эксплуатируемые информационные системы в образовательном учреждении, базы данных и традиционные хранилища данных, где присутствуют и обрабатываются персональные данные, определиться в каких информационных системах производится автоматизированная обработка, а где средства автоматизации (в понимании действующего законодательства) не используются.

Подготовить перечень необходимых организационных и технических мероприятий для обеспечения защиты:

- персональных данных, обрабатываемых без использования средств автоматизации;
- информационных систем, обрабатывающих персональные данные с использование средств автоматизации.

3. Формирование перечня персональных данных.

В целях выполнения норм Федерального закона «О персональных данных» (ст. 9 и ст. 14) необходимо сформировать перечень обрабатываемых персональных данных, так как:

- письменное согласие субъекта на обработку своих персональных данных должно включать в себя перечень персональных данных, на обработку которых дается согласие субъекта;
- субъект персональных данных имеет право на получение информации, касающейся обработки его данных, в том числе содержащей перечень обрабатываемых персональных данных и источник их получения.

4. Установление сроков обработки персональных данных.

Необходимо определить и зафиксировать документально предельные сроки хранения персональных данных после расторжения (прекращения) договора с работником, родителями учащихся, студентом и др. исходя из требований законодательства (в том числе гражданского, трудового, пенсионного, налогового, а также об исковой давности взаимных претензий образовательного учреждения и потребителя (заказчика) образовательных услуг и др.).

5. Ограничить доступ работников учреждения к персональным данным.

В целях обеспечения защиты персональных данных необходимо определить круг работников, которые допускаются к персональным данным работников, учащихся (воспитанников, студентов), а также категории предоставляемых им персональных данных.

Необходимо также наладить учет лиц, допущенных к работе с персональными данными в информационной системе, сформировать и утвердить списки

лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей.

В образовательном учреждении должны быть также:

- назначены ответственные за работу с персональными данными;
- уточнены должностные инструкции сотрудников, обрабатывающих персональные данные;
- обеспечена размещение и охрана средств хранения и обработки персональных данных.

6. Документально регламентировать работу с персональными данными

Требования трудового законодательства в отношении обработки персональных данных работника и гарантии их защиты устанавливают, что работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

Положение о защите персональных данных в образовательном учреждении является локальным актом образовательного учреждения, с которым, наряду Уставом учреждения и другими локальными актами необходимо знакомить родителей, законных представителей обучающихся (воспитанников), студентов.

7. Согласие субъектов персональных данных на обработку.

Необходимо оценить наличие предусмотренных законом оснований для обработки персональных данных без получения согласия субъекта персональных данных на их обработку. В случаях, когда такие основания отсутствуют, следует получить согласие субъекта персональных данных.

Целесообразно получить согласия работников и учащихся (родителей, законных представителей) на перевод части их персональных данных (например, ФИО, номер телефона, адрес e-mail) в категорию общедоступных.

Отдельный вопрос - передача персональных данных, где также в необходимых случаях получать согласие субъекта персональных данных на их передачу.

По мнению специалистов, цифровое фото относится к биометрическим персональным данным, поэтому в случае наличия в информационной системе образовательного учреждения фотографий работников, учащихся (воспитанников, студентов) также необходимо согласие на обработку биометрических персональных данных.

8. Пересмотр договоров с субъектами.

В целях упорядочения и облегчения получения согласий персональных данных рекомендуется пересмотреть договора с работниками и родителями учащихся, студентами в части обработки персональных данных и особенно их распространения (передачи).

9. Составление и направление в уполномоченный орган уведомления об обработке персональных данных.

Образовательное учреждений (орган управления образованием) В случае наличия оснований должен зарегистрироваться в качестве оператора персональных данных, для чего необходимо составить и направить в уполномоченный орган соответствующее уведомление.

Большинству образовательных учреждений этого делать не обязательно, особенно в случае получения согласий на обработку персональных данных. Образовательное учреждение вправе осуществлять без уведомления уполномоченного органа по защите прав субъектов персональных данных лишь обработку следующих персональных данных:

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения (работникам);
- полученных оператором в связи с заключением договора, стороной которого является субъект персональных данных (обучающийся и др.), если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта персональных данных и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом персональных данных;
- являющихся общедоступными персональными данными;

- включающих в себя только фамилии, имена и отчества субъектов персональных данных;

- необходимых в целях однократного пропуска субъекта персональных данных на территорию образовательного учреждения или в иных аналогичных целях;

-включенных в информационные системы персональных данных, имеющие в соответствии с федеральными законами статус федеральных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

- обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности персональных данных при их обработке и к соблюдению прав субъектов персональных данных.

Следующие шаги необходимо только при наличии в учреждении информационной системы персональных данных, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации. При этом образовательному учреждению следует оценить правовые основания работы с документами ДСП, качество собственной юридической службы (при ее наличии), перспективы судебных разбирательств и объем потенциальных санкций в случае признания судом методических документов ДСП, изданных ФСТЭК, обязательными для исполнения нормативными правовыми актами.

Подавляющему большинству образовательных учреждений нижеперечисленные шаги реализовывать нет необходимости.

10. Получение во ФСТЭК документов ДСП для выполнения требований действующего законодательства.

ФСТЭК России утвердило следующие документы ДСП, касающиеся защиты персональных данных:

- «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.

11. Формирование модели угроз персональным данным.

Определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз, исходя из утвержденной ФСТЭК базовой модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных, а также методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

12. Классифицирование информационных систем персональных данных.

Классификация информационных систем персональных данных, позволяющих осуществлять обработку персональных данных с использованием средств автоматизации, осуществляется образовательным учреждением - оператором в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20 в зависимости от категории обрабатываемых данных и их количества.

13. Приведение системы защиты персональных данных в соответствие с требованиями регуляторов.

В соответствии с Федеральным законом «О персональных данных» оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе 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.

14. Создание подсистем информационной безопасности информационных систем персональных данных и декларирование их соответствия, аттестация (сертификация).

Мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных предусматривают, что

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

- 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.

15. Получение лицензии на техническую защиту конфиденциальной информации.

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных, предусматривают, что операторы информационных системах персональных данных, проводя мероприятия по обеспечению безопасности персональных данных (конфиденциальная информация) при их обработке в информационных системах персональных данных 1-го и 2-го классов и распределенных информационных систем 3-го класса, должны получить лицензию ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации.

16. Организация эксплуатации информационных систем персональных данных и контроль за безопасностью.

Организация и поддержание системы защиты конфиденциальной информации от несанкционированного доступа осуществляется в соответствии с установленным классом информационной системы, с использованием средств защиты, сертифицированных в установленном порядке.

В соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя следующее:

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

- разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных.