**Защита персональных данных школьников и администрирование информационных систем школы**

Важнейшим компонентом системы является защита персональных данных школьников. В статье 3 федерального закона № 152 «О персональных данных» под персональными данными понимается «любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)».

Данная линия работы школы подчинена строгим правилам и находится в тесной взаимосвязи с нормативной базой. Для организации работы в этом направлении необходимо выполнение ряда шагов. Рассмотрим их.

Первым шагом является составление приказа о введении в действие документов, регламентирующих мероприятия по защите персональных данных (далее -ПДн).

Далее в целях обеспечения защиты персональных данных обрабатываемых в информационной системе персональных данных (далее - ИСПДн), необходимо утвердить и ввести в действие следующие организационно-распорядительные документы по защите персональных данных:

* Положение об обработке персональных данных в ИСПДн;
* Инструкция по обработке персональных данных, осуществляемых без использования средств автоматизации;
* Инструкция по обеспечению безопасности персональных данных, обрабатываемых в информационной системе персональных данных;
* Инструкция по организации парольной защиты;
* Инструкция ответственного за СЗИ ИСПДн;
* Инструкция по антивирусной защите;
* Форма согласия школьников и их родителей (законных представителей) на обработку их персональных данных;
* Перечень защищаемой информации;

Необходимо обеспечить ознакомление всех сотрудников с указанными документами.

Важным шагом является назначение ответственного за обработку персональных данных. Обычно таим человеком является заместитель директора по информатизации. Назначение ответственного сопровождается приказом директора. Приказ должен содержать следующую информацию: «С целью организации обработки персональных данных в ГБОУ СОШ …. в соответствии с пунктом 1 части 1 статьи 18.1 и части 1 статьи 22.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Требованиями к защите персональных данных при обработке в информационных системах персональных данных, утвержденными постановлением Правительства от 01.11.2012 № 1119, приказываю назначить ответственными за организацию обработки персональных данных…».

Сотрудник, ответственный за СЗИ ИСПДн, в пределах своих функциональных обязанностей организует обеспечение безопасности ПДн, обрабатываемых в ИСПДн с использованием средств автоматизации. Сотрудник руководствуется положениями Инструкции, разработанной учреждением, Приказа ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных», требованиями других нормативных правовых и нормативно–методических документов, регламентирующих защиту ПДн, при их автоматизированной обработке в ИСПДн, а также требованиями эксплуатационной документации на эксплуатируемые средства защиты информации, технические и программные средства, используемые в ИСПДн, имеющие встроенные механизмы защиты.

Основными функциями сотрудника ответственного за СЗИ ИСПДн являются:

* организация установки, сопровождения, администрирования и обеспечения функционирования средств и систем защиты информации в пределах возложенных на него обязанностей;
* обучение персонала и пользователей ИСПДн правилам работы со средствами защиты информации;
* организация определения и назначения прав пользователям ИСПДн на доступ к защищаемым информационным ресурсам ИСПДн в соответствии с Матрицей доступа, а также требованиями руководящих и нормативно–методических документов по защите ПДн;
* организация защиты всех критичных средств и информации, используемых для доступа в систему (паролей и идентификаторов);
* организация осуществления периодического контроля программной среды ИСПДн на отсутствие компьютерных вирусов;
* проведение периодического контроля состава штатного программного обеспечения (ПО) ИСПДн и их целостности;
* анализ журналов регистрации событий средств защиты от НСД;
* участие в проведении расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации в ИСПДн;
* текущий контроль технологического процесса обработки защищаемой информации в ИСПДн.

Каждым образовательным учреждением должна быть разработана политика обработки персональных данных, в том числе и данных обучающихся, включающая:

* общие положения;
* цели сбора персональных данных;
* правовые основания обработки персональных данных;
* объем и категории обрабатываемых персональных данных, категории субъектов персональных данных;
* порядок и условия обработки персональных данных;
* актуализация, исправление, удаление и уничтожение персональных данных, ответы на запросы субъектов персональных данных.

Политика обработки и защиты персональных данных (далее – ППД) определяет цели сбора, правовые основания, условия и способы обработки персональных данных, права и обязанности оператора, субъектов персональных данных, объем и категории обрабатываемых персональных данных и меры их защиты в ГБОУ.

Локальные нормативные акты и иные документы, регламентирующие обработку персональных данных в Образовательной организации, разрабатываются с учетом положений ППД. Действие ППД распространяется на персональные данные, которые Образовательная организация обрабатывает с использованием и без использования средств автоматизации.

Образовательная организация – оператор персональных данных – обязана:

1. Соблюдать конфиденциальность персональных данных, а именно не распространять персональные данные и не передавать их третьим лицам без согласия субъекта персональных данных или его законного представителя, если иное не предусмотрено законодательством.

2. Обеспечить субъектам персональных данных, их законным представителям возможность ознакомления с документами и материалами, содержащими их персональные данные, если иное не предусмотрено законодательством.

3. Разъяснять субъектам персональных данных, их законным представителям юридические последствия отказа предоставить персональные данные.

4. Блокировать или удалять неправомерно обрабатываемые, неточные персональные данные либо обеспечить их блокирование или удаление.

5. Прекратить обработку и уничтожить персональные данные либо обеспечить прекращение обработки и уничтожение персональных данных при достижении цели их обработки.

6. Прекратить обработку персональных данных или обеспечить прекращение обработки персональных данных в случае отзыва субъектом персональных данных согласия на обработку его персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, или иным соглашением между Образовательной организацией и субъектом персональных данных.

Далее необходимо организовать безопасное хранение персональных данных с помощью мер технической защиты, а также обучения персонала, имеющего доступ к персональным данным.