УТВЕРЖДЕНО
решением педсовета
БОУСОШ №6 МО Динской район
Протокол № 1 от 28.08.2014 г.
Директор _____ Н.Г. Хубанова

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в БОУСОШ №6 МО Динской район

I. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение об обеспечении безопасности персональных данных при обработке в информационной системе персональных данных (далее – Положение) БОУСОШ №6 МО Динской район (далее – ОО) разработано в соответствии с Постановлением Правительства РФ от 17.11.2007г. № 781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ОО, представляющих собой совокупность персональных данных, содержащихся в базах данных ОО, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

1.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства, средства защиты информации, применяемые в информационных системах.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ:

2.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу

(субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.2. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.4. Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.5. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

III. ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. 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.

3.2. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий

на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

3.4. Средства защиты информации, применяемые в информационных системах, в обязательном порядке проходят процедуру оценки соответствия в установленном законом порядке.

3.5. Информационные системы в БОУСОШ №6 классифицируются на основании приказа директора ОО, в соответствии с «Порядком проведения классификации информационных систем персональных данных», утвержденным приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

3.6. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

3.7. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

3.8. Безопасность персональных данных при их обработке в информационной системе персональных данных обеспечивает специалист, ответственный за обеспечение безопасности информационных систем персональных данных (администратор безопасности ИСПДн).

IV. ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

4.1. При обработке персональных данных в информационной системе должно быть обеспечено:

4.1.1. проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

4.1.2. своевременное обнаружение фактов несанкционированного доступа к персональным данным;

4.1.3. недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

4.1.4. возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

4.1.5. постоянный контроль над обеспечением уровня защищенности персональных данных.

4.2. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

4.2.1. определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

4.2.2. разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

4.2.3. проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

4.2.4. установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

4.2.5. обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

4.2.6. учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

4.2.7. учет лиц, допущенных к работе с персональными данными в информационной системе;

4.2.8. контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

4.2.9. разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

4.2.10. описание системы защиты персональных данных.

4.3. Осуществление мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе уполномоченным лицом возлагается на администратора безопасности ИСПДн БОУСОШ №6.

4.4. Список лиц, имеющих доступ к персональным данным, уполномоченных на обработку этих данных и несущих ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты персональных данных, утверждается приказом директора ОО.

4.5. Специалисты ОО, которым доступ к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей (далее – пользователи), для получения доступа к информационной системе направляют письменный запрос на имя ответственного за обеспечение безопасности персональных данных.

4.6. При обнаружении нарушений порядка предоставления персональных данных уполномоченное лицо незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

4.7. Иные требования по обеспечению безопасности информации и средств защиты информации в ОО выполняются в соответствии с требованиями федеральных органов исполнительной власти.