РАССМОТРЕНО
на заседании собрания
трудового коллектива
МБОУ «СОШ № 15»
протокол № 6 от 11.03.13г.

УТВЕРЖДЕНО
директором
МБОУ «СОШ № 15 »
О.А.Ефименковой
приказ № 99 от 12.03.13г.

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в МБОУ «Средняя общеобразовательная школа № 15 с углубленным изучением отдельных предметов» Энгельсского муниципального района Саратовской области

(новая редакция)

1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных МБОУ «Средняя общеобразовательная школа № 15 с углубленным изучением отдельных предметов» Энгельсского муниципального района Саратовской области (в дальнейшем –школа) представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее – информационные системы).

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 (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

2. 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.

Безопасность персональных данных при их обработке в информационных системах школы обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе 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 защиты должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности персональных данных при их обработке в информационных системах школы осуществляется защита речевой информации и

представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитооптической и иной основе.

3. Методы и способы защиты информации в информационных системах школы установлены в соответствии с требованиями Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации.

Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах школы оценивается при проведении государственного контроля и надзора.

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

5. Средства защиты информации, применяемые в информационных системах школы должны в установленном порядке проходить процедуру оценки соответствия.

6. Информационные системы школы классифицируются в структурных подразделениях, осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных, в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам работников школы, общества и государства в целом.

Порядок проведения классификации информационных систем школы должен соответствовать требованиям совместного Приказа Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации от 13 февраля 2008 года №55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

7. Обмен персональными данными при их обработке в информационных системах школы осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

8. Размещение информационных систем школы, 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.

9. Возможные каналы утечки информации при обработке персональных данных в информационных системах школы определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

10. Безопасность персональных данных при их обработке в информационной системе школы обеспечивают лица, которым на основании приказа директор школы поручает обработку персональных данных (далее – уполномоченное лицо). Существенным условием является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и их безопасность при обработке в информационной системе школы.

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

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

б) своевременное обнаружение факторов несанкционированного доступа к такой информации;

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

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль обеспечения уровня защищенности персональных данных.

12. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах школы включает в себя:

а) определение угроз безопасности персональных данных при их обработке и формирование на их основе частной модели угроз;

б) разработку на основе частной модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использование методов и способов защиты персональных данных, предусмотренных для третьего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключения о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационно–технической документацией;

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

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

ж) учет лиц, допущенных к работе с персональными данными в информационной системе;

з) контроль соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использование 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;

к) описание системы защиты персональных данных.

13. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе школы приказом директора уполномоченным лицом назначается ответственный за обеспечение безопасности персональных данных – Администратор безопасности информации.

14. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного директором школы.

15. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 14 настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется директором школы.

16. При обнаружении нарушений порядка предоставления персональных данных директор школы, ответственный за защиту информации персональных данных или уполномоченное лицо (администратор безопасности информации) незамедлительно приостанавливает предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

17. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

18. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их

обработке в информационных системах школы оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

19. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах школы прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

20. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах школы подлежат учету с использованием индексов или условных наименований и регистрационных номеров, которые определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.