УТВЕРЖДАЮ
Директор МБОУ СОШ № 23
_____М.Ю. Пименова
16 мая 2014 года

ТРЕБОВАНИЯ
по обеспечению безопасности персональных данных при обработке в информационной системе персональных данных (*сотрудники, учащиеся*)

1. Общие положения

Требования по обеспечению безопасности персональных данных (далее - Требования) при обработке в информационной системе персональных данных (*указать наименование системы*) (далее – ИСПДн) разработаны в целях исполнения Федерального Закона от 27 июля 2006 г. №152-ФЗ «О персональных данных». Под информационной системой персональных данных понимается информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

Требования разработаны на основании присвоенного ИСПДн класса, заданных характеристик безопасности, структуры ИСПДн, режима обработки персональных данных, режима разграничения прав доступа пользователей ИСПДн, местонахождения технических средств ИСПДн в соответствии с:

- Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781;

- Положением о методах и способах защиты информации в информационных системах персональных данных, утвержденным приказом Федеральной службы по техническому и экспортному контролю от 05 февраля 2010 года № 58.

2. Организационные требования по обеспечению безопасности персональных данных (далее – ПДн) при обработке в ИСПДн.

2.1. Должны быть определены:

- необходимость обработки персональных данных;
- перечень информации, подлежащей защите;
- конфигурация и топология ИСПДн, условия расположения данной ИСПДн относительно границ контролируемой зоны.
- технические средства и системы, предлагаемые к использованию в ИСПДн;
- перечень общесистемного и прикладного программного обеспечения, разрешенного к использованию в ИСПДн;

- перечень работников, допущенных к работе в ИСПДн и обработке ПДн;
- класс ИСПДн;
- угрозы безопасности ПДн в конкретных условиях функционирования;
- перечень используемых в ИСПДн средств защиты информации;
- планы организационно-технических мероприятий по защите информации;
- лица, ответственные за эксплуатацию средств защиты информации и обеспечение безопасности ПДн.

2.2. Должны быть разработаны и утверждены следующие организационно-распорядительные документы:

- требования по обеспечению безопасности ПДн при обработке в ИСПДн;
- приказ о назначении комиссии по определению и классификации ИСПДн;
- акт определения и классификации ИСПДн;
- модель угроз безопасности ПДн при их обработке в ИСПДн;
- инструкция администратора ИСПДн;
- инструкция пользователя ИСПДн;
- инструкция по проведению антивирусной защиты;
- инструкция по организации парольной защиты;
- инструкция по использованию установленных средств защиты информации от несанкционированного доступа;
- матрица доступа в ИСПДн;
- список лиц, допущенных к работе в ИСПДн;
- перечень программного обеспечения, разрешенного к использованию в ИСПДн;
- приказ о вводе в эксплуатацию ИСПДн;
- журнал учета и регистрации выдачи электронных носителей информации ИСПДн.

3. Требования по техническому обеспечению безопасности ПДн при обработке в ИСПДн (*устанавливаются на основе угроз безопасности в зависимости от класса ИСПДн, для примера приведены основные требования для ИСПДн 3-го класса при многопользовательском режиме обработки ПДн и равных правах доступа к ним*).

3.1. Требования к подсистеме управления доступом:

- должна осуществляться идентификация и проверка подлинности пользователя при входе в ИСПДн по идентификатору (коду) и паролю условно-постоянного действия длиной не менее 6-ти буквенно-цифровых символов.

3.2. Требования к подсистеме регистрации и учета:

- должна осуществляться регистрация входа (выхода) пользователя в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова, регистрация выхода из системы

или останова не проводится в моменты аппаратурного отключения информационной системы. В параметрах регистрации должны указываться дата и время входа (выхода) пользователя в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);

- должен осуществляться учет всех защищаемых носителей информации с помощью их маркировки и занесение учетных данных в журнал учета.

3.3. Требования к подсистеме обеспечения целостности:

– должна быть обеспечена целостность программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды, при этом целостность программных средств должна проверяться при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, а целостность программной среды должна быть обеспечена отсутствием в информационной системе средств разработки и отладки программ во время обработки и (или) хранения защищаемой информации;

– должна быть обеспечена физическая охрана информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения с установленной информационной системой посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации;

– должно осуществляться периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью специализированных тест-программ, имитирующих попытки несанкционированного доступа;

– должно быть обеспечено наличие средств восстановления системы защиты персональных данных, предусматривающее ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

Кроме того к основным требованиям могут быть прописаны дополнительные способы и методы защиты информации в конкретной ИСПДн

НАПРИМЕР:

3.4. Требования к подсистеме антивирусной защиты:

– должен быть организован непрерывный, согласованный по единому сценарию автоматический мониторинг информационного обмена в ИСПДн с целью выявления программно-математического воздействия (далее – ПМВ);

– должна проводиться автоматическая проверка на наличие вредоносных программ (программ-вирусов) и программных закладок;

– должны быть реализованы механизмы автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

– должна инициироваться автоматическая проверка ИСПДн на предмет наличия вредоносных программ при выявлении факта ПМВ;

– … (и др.)