



ПОЛОЖЕНИЕ

о порядке организации и проведения работ по защите персональных данных в МБОУ СОШ №43

1. Общие положения

1.1. Настоящее Положение разработано 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.

1.2. Настоящее Положение определяет порядок проведения организационно-технических мероприятий по защите персональных данных (далее - ПДн) в МБОУ СОШ №43 (далее учреждение)

2. Порядок определения защищаемой информации

2.1. Для определения защищаемой информации, а также информационных систем для ее обработки в учреждении создается комиссия.

2.2. Определение защищаемой информации проводится по результатам анализа всей имеющейся информации по каждому направлению деятельности учреждения.

2.3. Результаты работы комиссии отражаются в актах.

2.4. Для планирования, координации и проведения работ по защите информации ограниченного распространения в учреждении назначается уполномоченный по защите информации (далее - уполномоченный).

3. Порядок привлечения и задачи структурных подразделений и специалистов учреждения, специализированных сторонних организаций к созданию информационных систем

3.1 Для создания информационных систем персональных данных (далее ИСПДн) и разработки системы защиты информации (далее СЗИ) привлекается структурное подразделение учреждения, для которого создаются ИСПДн.

3.2 Для создания ИСПДн и разработки СЗИ допускается в установленном законодательством порядке привлечение на договорной основе специализированных организаций, имеющих лицензии ФСБ России и ФСТЭК России на соответствующий вид деятельности в области защиты конфиденциальной информации.

3.3 Организация и проведение работ на всех стадиях создания и эксплуатации ИСПДн возлагается на руководителя структурного подразделения учреждения, которое будет осуществлять эксплуатацию ИСПДн (далее – структурное подразделение), и уполномоченного.

3.4 Разработка и создание СЗИ в ИСПДн возлагается на уполномоченного.

3.5 Все действия, связанные с привлечением сторонних организаций к средствам обработки защищаемой информации, должны быть основаны на договорных отношениях и обеспечивать конфиденциальность обрабатываемой информации.

4. Порядок взаимодействия структурных подразделений при проведении работ по созданию ИСПДн

4.1 Деятельность структурных подразделений и специалистов учреждения по созданию ИСПДн осуществляется в соответствии с требованиями федеральных и краевых нормативных правовых актов, внутренних документов учреждения в области защиты информации. Координацию работ по созданию ИСПДн осуществляет уполномоченный.

4.2 В случае возникновения необходимости создания ИСПДн руководитель структурного подразделения информирует об этом уполномоченного для совместного принятия решения о последующем порядке действий.

4.3 Предложения о создании ИСПДн выносятся уполномоченными совместно с руководителем структурного подразделения на рассмотрение руководству.

4.4 Уполномоченный совместно с руководителем структурного подразделения приступают к работе по созданию ИСПДн после принятия руководством окончательного решения и утверждения плана работы по данному вопросу.

5. Порядок разработки, ввода в действие и эксплуатации ИСПДн

5.1 Предпроектная стадия.

5.1.1 Предпроектное обследование автоматизированных систем (далее - АС) проводится уполномоченным совместно со специалистами структурного подразделения, которые участвуют в определении (уточнении):

— угроз безопасности информации применительно к конкретным условиям функционирования;

— конфигурации, топологии АС и систем в целом, а также их отдельных компонентов;

— физических, функциональных и технологических связей как внутри этих систем, так и с другими системами различного уровня;

— режима обработки информации в АС в целом и в ее отдельных компонентах;

— средств вычислительной техники и связи, технических и программных средств, предназначенных для обработки защищаемой информации.

5.2 Класс информационных систем персональных данных устанавливается в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденных приказом ФСБ России, ФСТЭК России и Мининформсвязи России от 13 февраля 2008г. №55/86/20 и оформляется актом.

5.3 При необходимости разработки технического проекта на ИСПДн уполномоченным совместно с сотрудниками структурного подразделения разрабатывается техническое (частное техническое) задание с учетом установленного класса ИСПДн.

5.4 Стадия проектирования и создания ИСПДн.

5.4.1 Разработка технического проекта на ИСПДн и СЗИ в его составе по решению руководителя учреждения проводится специализированной организацией, имеющей лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, или уполномоченным совместно с сотрудниками структурного подразделения.

5.4.2 На основе требований, определенных при предпроектном обследовании, учреждением осуществляется закупка сертифицированных по требованиям безопасности технических и программных средств защиты, обработки и хранения информации.

5.4.3 На стадии создания ИСПДн уполномоченным совместно со специалистами структурного подразделения осуществляются организационные и технические мероприятия по защите информации:

- размещение и монтаж технических средств и систем обработки конфиденциальной информации;
- организация охраны и физической защиты помещений с установленной ИСПДн в целях исключения несанкционированного доступа к техническим средствам обработки, хранения и передачи информации, нарушения их работоспособности, хищения средств и носителей информации;
- определение лиц, ответственных за эксплуатацию средств защиты информации;
- обучение лиц, назначенных ответственным за эксплуатацию ИСПДн, специфике работы с учетом требований по безопасности информации и установленного класса;
- разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;
- разработка организационно-распорядительной документации в ИСПДн.

5.5 Стадия ввода в эксплуатацию ИСПДн.

5.5.1 Специалистами структурного подразделения совместно с уполномоченным на стадии ввода в эксплуатацию ИСПДн и СЗИ проводится проверка работоспособности средств защиты информации в комплексе с другими техническими и программными средствами в составе ИСПДн и отработка технологического процесса обработки (передачи) информации.

5.5.2 Ввод ИСПДн в эксплуатацию осуществляется после проведения его комплексной проверки (аттестационных испытаний) в реальных условиях эксплуатации в целях оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

5.5.3 ИСПДн вводится в эксплуатацию приказом учреждения.

5.5.4 Эксплуатация ИСПДн осуществляется специалистами структурного подразделения в соответствии с условиями и требованиями, определенными внутренними организационно-распорядительными документами учреждения по защите информации и утвержденным техническим паспортом на ИСПДн.

5.5.5 Внесение специалистами структурных подразделений самостоятельных несогласованных изменений в технологическую, аппаратную и программную конфигурацию ИСПДн не допускается.

5.5.6 Все изменения в информационных технологиях обработки информации в ИСПДн, составе и размещении технических средств и систем, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации в ИСПДн согласуются с уполномоченным.

5.5.7 Для своевременного выявления и предотвращения утечки информации по техническим каналам, исключения несанкционированного доступа и предотвращения специальных программно-технических воздействий, вызывающие нарушение целостности информации или работоспособности технических средств, проводится периодический контроль состояния защиты информации.

Контроль осуществляется уполномоченным (не реже одного раза в квартал) и заключается в оценке:

- соблюдения требований нормативных и методических документов ФСТЭК России;

- работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

- выполнении специалистами структурного подразделения своих обязанностей в части обеспечения защиты информации.

5.5.8 В целях исключения возможных последствий специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности технических средств обработки, хранения и защиты информации (не реже одного раза в квартал).

5.5.9 Все съемные машинные носители информации, задействованные при эксплуатации ИСПДн регистрируются уполномоченным в Журнале регистрации и учета электронных носителей информации для предотвращения утечки информации по техническим каналам, исключения несанкционированного доступа. Использование в ИСПДн специалистами неучтенных съемных носителей информации не допускается.

5.5.10 При выявлении в ходе проведения контроля нарушения правил эксплуатации ИСПДн, технологии обработки защищаемой информации и требований по безопасности информации эксплуатация ИСПДн может быть приостановлена решением руководителя до момента восстановления требуемого уровня безопасности информации.

5.5.11 Результаты проводимого контроля отражаются в техническом паспорте на ИСПДн.

6. Ответственность должностных лиц структурных подразделений, занятых в создании и эксплуатации ИСПДн

6.1 Ответственность за своевременность подачи информации о необходимости создания ИСПДн для обработки защищаемой информации возлагается на руководителя структурного подразделения.

6.2 Ответственность за качество формирования требований по технической защите конфиденциальной информации при создании ИСПДн, а также за полноту и качество разработки системы защиты информации в его составе возлагается на уполномоченного.

6.3 Должностные лица структурного подразделения несут ответственность за выполнение требований по безопасности информации, соблюдение технологии обработки защищаемой информации, неизменность условий обработки информации (размещение и/или состав технических средств обработки и защиты информации, состав используемого в ИСПДн программного обеспечения) в соответствии с организационно-технической документацией на эксплуатируемую ИСПДн.

6.4 При нарушении требований по безопасности информации на должностных лиц учреждения налагается дисциплинарная и административная ответственность в соответствии с действующим законодательством Российской Федерации.