СОГЛАСОВАНО:
Председатель первичной профсоюзной организации ГБОУ «СКШ № 2»
_____ Т.В. Кочеткова
«13» ноября 2014 г.

УТВЕРЖДАЮ:
Директор ГБОУ «СКШ № 2»
_____ В.В. Богданов
«13» ноября 2014 г.

Положение
по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Государственного бюджетного общеобразовательного учреждения Саратовской области «Саратовская кадетская школа-интернат № 2»

1. Назначение документа

Настоящий документ определяет порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн Государственном бюджетном общеобразовательном учреждении Саратовской области «Саратовская кадетская школа-интернат № 2» и содержит общие принципы защиты ПДн.

Данный документ направлен на достижение следующих целей:

- выполнение требований законодательства в области обеспечения безопасности ПДн;
- защита прав и свобод граждан РФ при обработке их ПДн в ИСПДн оператора;
- защита ПДн, обрабатываемых оператором, от НСД и от других несанкционированных действий.

2. Область действия

Требования настоящего Положения распространяются на все подразделения оператора, которые участвуют в обработке ПДн, либо в организации обработки ПДн, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение функционирования ИСПДн.

Настоящий документ обязаны знать и использовать в работе все сотрудники оператора, а также другие лица, допущенные к работе в ИСПДн.

3. Общие положения

Настоящее Положение устанавливает требования по защите ПДн, принципы обработки ПДн в ИСПДн оператора.

Настоящее Положение разработано в соответствии со следующими нормативными актами:

- Федеральным законом Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных»;
- Федеральным законом Российской Федерации от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановлением Правительства Российской Федерации от 15 сентября 2008 г. №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке

в информационных системах персональных данных»;

– Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– методическими документами ФСБ России, ФСТЭК России, Роскомнадзора.

Настоящее Положение является методологической основой для:

– формирования и проведения единой политики в области обеспечения безопасности ПДн;

– принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технического и организационно-технического характера, направленных на выявление, отражение и уменьшение УБПДн;

– координации деятельности при проведении работ по созданию, развитию и эксплуатации ИСПДн с соблюдением требований по обеспечению безопасности ПДн;

– разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн.

Принципы и требования по обеспечению безопасности ПДн распространяются:

– на все возможные формы существования информации, такие как:

физические поля (электрические, акустические, электромагнитные, оптические и т.п.);

носители на бумажной, магнитной, оптической и иной основе.

– на все возможные форматы представления ПДн, такие как:

- документы;
- голос;
- изображения;
- файлы;
- почтовые сообщения;
- базы данных;
- записи базы данных;
- другие информационные массивы.

Предотвращение несанкционированного и нелегитимного доступа к ИСПДн, технологиям и информационным ресурсам результатом которого может стать уничтожение, модификация, искажение, копирование, распространение, блокирование ПДн требует применения комплекса правовых, организационных, организационно-технических мер защиты с использованием сертифицированных СЗИ.

Настоящее Положение определяет:

– роли, полномочия, ответственность за обеспечение безопасности ПДн, подразделений оператора;

– порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн;

– мероприятия по обеспечению безопасности ПДн;

– требования по управлению процессом обеспечения безопасности ПДн;

– требования к составу и содержанию документов оператора, регламентирующих защиту и работу с ПДн.

Целью создания СЗПДн является исключение неправомерного или случайного доступа к ПДн, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий.

В общем случае можно выделить следующие основные цели защиты ПДн, это обеспечение:

- конфиденциальности ПДн;
- целостности ПДн;
- доступности ПДн;
- неотказуемости.

Конкретный состав целей защиты ПДн зависит от конкретной ИСПДн и определяется по результатам разработки модели угроз и нарушителя безопасности ПДн.

К основным задачам в области обеспечения безопасности ПДн относится:

- определение новых ИСПДн;
- инвентаризация и управление изменениями в составе и структуре ИСПДн;
- сбор согласий на обработку ПДн с субъектов ПДн;
- разработка и актуализация Перечня сведений конфиденциального характера;
- уничтожение ПДн;
- управление взаимодействиями с внешними контрагентами по вопросам обработки ПДн;
- взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- определение уровня защищенности ИСПДн;
- разработка (актуализация) документации на СЗПДн;
- выбор и внедрение необходимых и достаточных мер и средств защиты ПДн;
- эксплуатация СЗПДн в соответствии с документацией на нее;
- контроль уровня защищенности ПДн;
- обучение персонала по вопросам защиты ПДн;
- учет применяемых СЗИ, эксплуатационной и технической документации к ним, носителей ПДн;
- учет лиц, допущенных к обработке ПДн;
- взаимодействие с регуляторными органами по вопросам защиты ПДн;
- актуализация и подача уведомлений в уполномоченный орган по защите прав субъектов ПДн;
- аттестация (декларирование соответствия) по требованиям безопасности информации;
- получение лицензий ФСТЭК России и ФСБ России в области защиты ПДн.

Обработка ПДн должна осуществляться в соответствии со следующими принципами:

- законности целей и способов обработки ПДн и добросовестности;
- соответствия целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора;
- соответствия объема и характера обрабатываемых ПДн, способов обработки ПДн целям обработки ПДн;
- достоверности ПДн, их достаточности для целей обработки, недопустимости обработки ПДн, избыточных по отношению к целям, заявленным при сборе ПДн;
- недопустимости объединения созданных для несовместимых между собой целей баз данных ИСПДн.

Оператор должен проводить регулярный анализ соответствия процессов обработки ПДн указанным принципам. Данный анализ проводится в случае:

- создания новых ИСПДн;
- внесения изменений в технологические процессы существующие в ИСПДн;
- изменения нормативной базы затрагивающей принципы и (или) процессы обработки ПДн в ИСПДн оператора;
- проведения контрольных и проверочных мероприятий на предмет оценки соответствия процессов обработки ПДн заявленным принципам.

Отнесение сведений оператором к ПДн, безопасность которых должна

обеспечиваться СЗПДн представляет собой процесс обоснованного установления (документального оформления и утверждения) критериев их выделения из всей совокупности сведений, находящихся в обращении.

В качестве такого критерия у оператора разрабатывается и утверждается Перечень персональных данных, подлежащих защите в Государственном бюджетном общеобразовательном учреждении Саратовской области «Саратовская кадетская школа-интернат № 2».

4. Организационная структура системы защиты персональных данных

СЗПДн является частью общей системы обеспечения информационной безопасности оператора.

Основу организационной структуры СЗПДн как правило составляют следующие организационные структуры:

- руководство;
- ответственные за обеспечение безопасности ПДн;
- администраторы безопасности ИСПДн;
- ответственные за техническое сопровождение ИСПДн;
- структурные подразделения, участвующие в процессах обработки ПДн;
- сотрудники оператора.

Руководство осуществляет следующие основные функции в области обеспечения безопасности ПДн:

- обеспечивает общую организацию работ по защите ПДн;
- издает приказы по вопросам организации СЗПДн;
- утверждает Перечень сведений конфиденциального характера;
- назначает ответственных за обеспечение безопасности ПДн;
- утверждает список лиц, допущенных к обработке ПДн;
- рассматривает и утверждает нормативные документы оператора, регламентирующие обработку и защиту ПДн;
- заслушивает при необходимости ответственных за обеспечение безопасности ПДн и других должностных лиц о состоянии работ по защите ПДн.

Ответственные за обеспечение безопасности ПДн осуществляют следующие основные функции:

- разрабатывают Перечень сведений конфиденциального характера;
- участвуют в проведении определении уровня защищенности ИСПДн;
- распределяют ответственность по вопросам обработки и защиты ПДн;
- определяют допустимые сроки хранения ПДн по каждой категории ПДн;
- организуют подачу уведомлений в уполномоченный орган по защите прав субъектов ПДн;
- заслушивают руководителей структурных подразделений о принимаемых мерах по состоянию и совершенствованию СЗПДн;
- организуют работы по разработке, изменению и уточнению политик, регламентов, стандартов в части защиты ПДн;
- осуществляют организацию плановых и внеплановых проверочных мероприятий;
- организуют выполнение требований по защите ПДн у оператора;
- проводят разработку и актуализацию локальных нормативных документов, регламентирующих защиту ПДн у оператора;
- проводит ознакомление сотрудников с нормативными документами в области защиты ПДн;
- проводят оценку эффективности принятых мер и применяемых средств защиты ПДн;
- проводят занятия с сотрудниками по изучению организационно-

распорядительных документов по всему комплексу вопросов защиты ПДн;

– разрабатывают и актуализируют частные модели угроз безопасности ПДн и технические задания на СЗПДн;

– определяют необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, а также определяют формы и программы обучения сотрудников оператора в области защиты ПДн;

– контролируют выполнение сотрудниками требований по защите ПДн;

– организуют работы по сбору сведений об изменениях в составе и структуре ИСПДн;

– осуществляют контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов по защите ПДн, а также внутренних организационно-распорядительных документов оператора;

– контролируют исполнение требований по уничтожению ПДн;

– разрабатывают рекомендации по оптимизации существующих и новых информационных процессов обработки ПДн по критериям соответствия требованиям по защите ПДн и минимизации затрат на создание и эксплуатацию системы защиты ПДн;

– контролируют исполнение требований нормативных документов оператора в области обеспечения безопасности ПДн, структурными подразделениями и сотрудниками;

– организуют и осуществляют взаимодействие с регуляторами по вопросам защиты ПДн;

– участвуют в аттестации (декларировании соответствия) ИСПДн оператора по требованиям безопасности информации;

– управляют проектами по внедрению систем и средств защиты ПДн;

– контролируют ввод в действие, эксплуатацию СЗПДн;

– проводят расследования инцидентов, связанных с нарушением безопасности ПДн, правил обработки ПДн, принимают меры по недопущению повторения нештатных ситуаций.

Администраторы безопасности ИСПДн осуществляют следующие основные функции:

–осуществляют сопровождение средств и систем защиты ПДн;

–проводят оперативный контроль функционирования средств и систем защиты ПДн;

–проводят резервирование ПДн;

–ведут учет носителей ПДн;

–осуществляют выявление и регистрацию попыток НСД к компонентам ИСПДн, информационным ресурсам;

– контролируют соответствие технических, программных и программно-аппаратных средств ИСПДн требованиям, предъявляемым к ним средствами и СЗПДн;

– осуществляют учет применяемых СЗИ, эксплуатационной и технической документации к ним;

– контролируют выполнение сотрудниками подразделения требований по защите ПДн;

– участвуют в расследованиях причин возникновения нештатных ситуаций;

– готовят предложения по совершенствованию СЗПДн;

– выполняют комплекс мероприятий по защите информации при проведении ремонтных и регламентных работ;

– обеспечивают защиту ПДн при выводе из эксплуатации компонентов ИСПДн.

Ответственные за техническое сопровождение ИСПДн осуществляют следующие основные функции:

– осуществляют сопровождение технических средств и систем ИСПДн.

Структурные подразделения, участвующие в процессах обработки ПДн выполняют следующие основные функции:

- осуществляют взаимодействие с субъектами ПДн по вопросам обработки их ПДн;
- осуществляют уведомление субъектов ПДн в случаях определенных нормативными актами;
- эксплуатируют СЗПДн в соответствии с документацией на нее.

Сотрудники оператора выполняют следующие основные функции:

- соблюдают требования нормативных документов по защите ПДн;
- осуществляют обработку ПДн в соответствии с заданием и предоставленными полномочиями.

Конкретное распределение функций администраторов безопасности, ответственных за техническое сопровождение ИСПДн, сотрудников должно быть приведено в должностных инструкциях.

Распределение ролей, полномочий осуществляется в соответствии с Разрешительной системой доступа к информационным ресурсам, программным и техническим средствам информационных систем персональных данных.

5. Порядок организации и проведения работ по обеспечению безопасности персональных данных

Работы по обеспечению безопасности ПДн при их обработке в ИСПДн являются неотъемлемой частью работ выполняемых в рамках жизненного цикла ИСПДн, на следующих этапах:

- инициация проекта ИСПДн;
- планирование проекта ИСПДн;
- реализация проекта ИСПДн, в составе:
- выбор технического решения - концепция реализации;
- проектирование ИСПДн;
- производство ИСПДн;
- приемка ИСПДн;
- внедрение ИСПДн;
- передача системы в эксплуатацию;
- документирование проекта.
- эксплуатация ИСПДн;
- модернизация ИСПДн;
- вывод из эксплуатации.

6. Допуск персонала к обработке персональных данных

При допуске к ПДн оператор руководствуется утвержденным списком лиц, допущенных к обработке ПДн.

Перечень лиц, допущенных к обработке ПДн, составляется и корректируется ответственными за обеспечение безопасности ПДн, на основании данных подаваемых руководителями структурных подразделений оператора.

7. Контроль изменений в составе и структуре информационных систем персональных данных

Все изменения в составе и структуре ИСПДн должны контролироваться и регламентироваться ответственными за обеспечение безопасности ПДн.

Контролю подлежат следующие изменения:

- внесение новых устройств в состав ИСПДн (АРМ, серверов, сетевого и телекоммуникационного оборудования и т.п.);
- изменение мест включения существующих компонент ИСПДн;

- удаление устройства из состава ИСПДн;
- изменение мест установки устройства из состава ИСПДн;
- прокладка новых кабельных линий связи и внешних линий связи или удаление старых кабельных линий связи;
- существенное изменение состава и конфигурации системного и прикладного программного обеспечения, участвующего в обработке ПДн;
- создание новых и изменение существующих технологических процессов связанных с обработкой ПДн.

Каждое изменение состава ИСПДн, типов технических средств, топологии ИСПДн должно отслеживаться и анализироваться на предмет соответствия требованиям по защите ИСПДн. При необходимости должна производиться модернизация СЗПДн.

8. Защита от несанкционируемого доступа к элементам информационных систем персональных

Мероприятия по физическому контролю доступа включают:

- мероприятия по контролю доступа на территорию;
- мероприятия по контролю доступа в помещения с оборудованием ИСПДн;
- мероприятия по контролю доступа к техническим средствам ИСПДн;
- мероприятия по контролю перемещений физических компонентов ИСПДн.

Мероприятия по контролю доступа на территорию должны обеспечить контролируемое нахождение посетителей на территории оператора.

Помещения с серверным, телекоммуникационным и сетевым оборудованием ИСПДн должны иметь прочные входные двери с надежными кодовыми замками или приспособлениями для опечатывания. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей ИСПДн, должны быть оборудованы замками, либо в этих помещениях должны обеспечиваться мероприятия по контролю действий находящихся в них посторонних лиц.

Нахождение в помещении лиц, не участвующих в технологических процессах обработки ПДн (обслуживающий персонал, другие сотрудники), должно производиться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не допущенными к обработке ПДн.

При выносе устройств, хранящих ПДн, за пределы КЗ для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации хранимой на этих устройствах.

9. Резервирование персональных данных

Резервирование ПДн должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

Резервированию должна подвергаться информация на серверах ИСПДн.

Резервирование должно осуществляться на различные носители информации с соответствующим уровнем надежности и долговечности.

Хранение резервных копий должно осуществляться в надежных сейфах (металлических шкафах). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

Доступ к резервным копиям должен быть строго регламентирован.

10. Контроль за обеспечением необходимого уровня защищенности персональных данных

Для обеспечения эффективности процесса обеспечения безопасности ПДн проводится:

- контроль за соблюдением требований по обработке и защите ПДн;
- контроль за соблюдением условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- контроль эффективности средств защиты ПДн.

Контрольные мероприятия могут быть:

- текущими;
- внезапными;
- плановыми внешними;
- плановыми внутренними.

Ответственность за текущий контроль эффективности обеспечения безопасности ПДн возлагается на администраторов безопасности ИСПДн.

Ответственность за плановый контроль эффективности обеспечения безопасности ПДн возлагается на ответственных за обеспечение безопасности ПДн. Данные проверки должны включаться в план аудитов информационной безопасности на год.

Для планового контроля эффективности СЗПДн должны использоваться средства выявления уязвимостей информационной безопасности.

Внезапные проверки эффективности при необходимости могут проводиться специальными группами по решению ответственных за обеспечение безопасности ПДн.

При проведении контроля эффективности в общем случае должно проверяться:

- наличие установленных СЗИ;
- корректность настроек СЗИ;
- выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;
- исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
- правильность организации работы с носителями ПДн;
- правильность обращения ключевой информации;
- соответствие СЗПДн реальному положению дел у оператора.

11. Реагирование на нештатные ситуации

Оператор должен проводить расследования инцидентов, связанных с НСД и другими несанкционированными действиями затрагивающими безопасность ПДн.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью ПДн;
- ликвидация последствий инцидентов связанных с безопасностью ПДн;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.